# CA Access Control

# 故障排除指南

12.8

# 第三方通知

# 示例脚本和示例 SDK 代码

CA Access Control 产品随附的示例脚本和示例 SDK 代码均“按原样”提供，仅供参考之用。在特定环境下，可能需要对它们进行调整，而且在生产系统中部署它们之前，未经事先测试和验证不应将其用于生产。

CA Technologies 不向这些示例提供支持，而且对于这些脚本可能会引起的任何错误概不负责。

# CA Technologies 产品引用

本文档引用以下 CA Technologies 产品：

- CA Access Control
- CA Access Control
- CA Single Sign-On (CA SSO)
- CA Top Secret®
- CA ACF2™
- CA Audit
- CA Network and Systems Management（CA NSM，以前为 Unicenter NSM 和 Unicenter TNG）
- CA Software Delivery（以前为 Unicenter Software Delivery）
- CA Service Desk（以前为 Unicenter Service Desk）
- CA User Activity Reporting Module（以前是 CA Enterprise Log Manager）
- Identity Manager

# 文档约定

CA Access Control 文档使用以下约定：

| 格式 | 含义 |
| --- | --- |
| 等宽字体 | 代码或程序输出 |
| *斜体* | 重点或新术语 |
| **粗体** | 必须完全按照显示内容键入的文本 |
| 正斜杠 (/) | 用于描述 UNIX 和 Windows 路径的独立于平台的目录分隔符 |

文档在解释命令语法和用户输入（以等宽字体显示）时还会使用以下特殊约定：

| 格式 | 含义 |
| --- | --- |
| *斜体* | 您必须提供的信息 |
| 用方括号括起来 ([]) | 可选运算符 |

| 格式 | 含义 |
| --- | --- |
| 用大括号括起来 ({}) | 强制运算符集 |
| 用管道符（\|）分隔的选项。 | 分隔可选运算符（选择一项）。<br>例如：下面的示例*既*可以表示用户名，*也*可以表示组名：<br>`{username\|groupname}` |
| ... | 指明前面的项或项组可以重复 |
| 下划线 | 默认值 |
| 前面带空格的行尾反斜杠 ( \) | 有时，在本指南中，一行无法容纳一个命令。在这些情况下，行结尾处的空格加上反斜杠 ( \) 就表示该命令延续到下一行。<br>**注意：**请勿复制反斜杠字符，并且请省略换行符。这些不是实际命令语法的一部分。 |

### 示例：命令表示法约定

下面的代码说明了在本指南中使用命令约定的方式：

```
ruler className [props({all|{propertyName1[,propertyName2]...})]
```

在该示例中：

- 命令名称 (ruler) 以常规等宽字体显示，必须按照显示内容键入。
- *className* 选项以斜体显示，因为它是一个类名（例如 USER）的占位符。
- 即使不带有方括号中的第二部分，您也可以运行该命令，方括号表示该运算符是可选的。
- 使用可选参数 (props) 时，可以选择关键字 *all*，也可以指定一个或多个属性名（以逗号分隔）。

## 文件位置约定

CA Access Control 文档使用以下文件位置约定：

- *ACInstallDir*—默认 CA Access Control 安装目录。
  - Windows—C:\Program Files\CA\AccessControl\
  - UNIX—/opt/CA/AccessControl/
- *ACSharedDir*—CA Access Control for UNIX 使用的默认目录。
  - UNIX—/opt/CA/AccessControlShared

- *ACServerInstallDir*—默认 CA Access Control 企业管理 安装目录。
  - /opt/CA/AccessControlServer
- *DistServerInstallDir*—默认分发服务器安装目录。
  - /opt/CA/DistributionServer
- *JBoss_HOME*—默认 JBoss 安装目录。
  - /opt/jboss-4.2.3.GA

# 联系技术支持

要获取在线技术帮助以及办公地址、主要服务时间和电话号码的完整列表，请联系技术支持：http://www.ca.com/worldwide。

# 文档更改

从最新版本以来对该文档进行了以下更新：

- 缺少对于 Linux 安装而言必需的程序包
- MALLOC_ARENA_MAX=1 未在 RedHat Linux 6.2 上工作
- 由于不正确参数，无法创建端点
- PUPM 导送程序轮询在负载平衡环境中不一致

# 目录

# 第 1 章： 简介

此部分包含以下主题：



## 关于本指南

本指南为您在使用 CA Access Control 时可能遇到的一些常见问题提供了解决方案和变通方法。

为了简化术语，在本指南中我们将此产品称为 CA Access Control。

## 使用本指南的用户

本指南的目标读者是在实施、配置和维护受 CA Access Control 保护的环境时遇到问题的安全管理员和系统管理员。

# 第 2 章： 安装 CA Access Control 端点和服务器组件

此部分包含以下主题：

# 为 JDK 1.7 配置 Java 连接器服务器

**症状：**

我需要完成哪些修改才能在企业管理服务器上支持 JDK 1.7 U17。

**解决方案：**

要在企业管理服务器上支持 JDK 1.7 U17，您必须修改 Java 连接器服务器 (JCS)。请执行以下操作：

### Windows 2008 Server 32 位操作系统

1. 在命令行窗口中，运行 regedit。

   此时将打开“注册表编辑器”。

2. 导航到以下位置：

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\Identity
   Manager\Procrun 2.0\im_jcs\Parameters
   ```

3. 选择环境注册表项并按如下方式修改值：

   ```
   PATH=%PATH%;C:\Program Files\Java\jdk1.7.0_17\jre\bin
   ```

4. 导航到以下位置：

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\Identity
   Manager\Procrun 2.0\im_jcs\Parameters\Java
   ```

5. 选择 jvm 注册表项并按如下方式修改值：

   ```
   C:\Program Files\Java\jdk1.7.0_17\jre\client\jvm.dll
   ```

### Windows 2008 Server R2 64 位操作系统

1. 在命令行窗口中，运行 regedit。

   此时将打开“注册表编辑器”。

2. 导航到以下位置：

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Computer
   Associates\Identity Manager\Procrun 2.0\im_jcs\Parameters
   ```

3. 选择环境注册表项并按如下方式修改值：

   ```
   PATH=%PATH%;C:\Program Files (x86)\Java\jdk1.7.0_17\jre\bin
   ```

4. 导航到以下位置：

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Computer
   Associates\Identity Manager\Procrun
   2.0\im_jcs\Parameters\Java
   ```

5. 选择 jvm 注册表项并按如下方式修改值：

   ```
   C:\Program Files
   (x86)\Java\jdk1.7.0_17\jre\bin\client\jvm.dll
   ```

### Red Hat Linux x64 操作系统

1. 删除所有指向 JDK 的现有链接。
2. 确认 Java 连接器服务器未运行。
3. 更改 /usr/bin/java 链接以指向 Java 7。如以下示例所示：

```
# ln -s /opt/Java/jdk1.7.0_17/bin/java /usr/bin/java
# ln -s /opt/Java/jdk1.7.0_17/bin/java /bin/java

# ls -l /usr/bin/java
lrwxrwxrwx 1 root root 30 Apr  8 12:05 /usr/bin/java ->
/opt/Java/jdk1.7.0_17/bin/java
# which java
/usr/bin/java
```

4. 删除以下目录：
   `/opt/CA/AccessControlServer/Connector_Server/jvm`
5. 启动 Java 连接器服务器。
   `./im_jcs.new start`

# 缺少对于 Linux 安装而言必需的程序包

**症状：**

安装失败，因为缺少必需的 Linux 程序包。

**解决方案：**

使用 rpm --requires 和 rpm --whatprovides 命令来确认程序包依存关系，并安装缺少的程序包。

**注意**：有关所需程序包的详细信息，请参阅《*CA Access Control 版本说明*》的“安装注意事项”部分中的“在 Red Hat Linux 6 上安装企业管理服务器所需的 32 位程序包”。

## rpm --requires－检测库依存关系

在 Linux 上安装企业管理时，您需要知道 CAeAC 程序包依赖哪些库。

该命令使用以下语法：

```
rpm -qp --requires package
```

该命令具有以下参数：

**-q**

指定您想要查询 RPM 程序包信息。

**-p**

查询 RPM 程序包文件。同时检索有关未安装的程序包的信息。

**--requires *package***

检索程序包需要的依存关系。

### 示例

您想要检索有关 CA Access Control 12.8 SP0 的依存关系信息。

```
root> rpm -qp --requires CAeAC-1280-0.0.1275.i386.rpm
rpm >= 4.0
libcrypt.so.1
libc.so.6
libdl.so.2
libgcc_s.so.1
libm.so.6
libnsl.so.1
libpam.so.0
libpthread.so.0
libresolv.so.2
libstdc++.so.6
rpmlib(PayloadFilesHavePrefix) <= 4.0-1
rpmlib(CompressedFileNames) <= 3.0.4-1
```

继续在列出的程序包上逐个运行 rpm 命令以检索进一步的依存关系。

```
root> rpm -qp --requires libcrypt
```

**更多信息：**

rpm --whatprovides－确认库存在 (p. 19)

## rpm --whatprovides－确认库存在

在 Linux 上安装企业管理之前，请确认目标系统上已包含所有必需的库。

该命令使用以下语法：

```
rpm -q --whatprovides capability
```

该命令具有以下参数：

**-q**

指定您想要查询 RPM 程序包信息。

**--whatprovides *capability***

指定您想要检索哪个程序包提供该功能的信息。

### 示例：确认库已安装

在本示例中，您想要确认 libcrypt.so.1 已安装。您将收到肯定回答（$? 为 0），并且了解到 libcrypt.so.1 是由 glibc-2.5-42 程序包提供的。

```
root> rpm -q --whatprovides libcrypt.so.1
glibc-2.5-42
root> echo $?
0
```

### 示例：检测到库未安装

在本示例中，您想要找出 libexample.so.1 是否已安装。您将收到否定回答（$? 为 1），因为未安装提供此功能的程序包。

```
root> rpm -q --whatprovides libexample.so.1
no package provides libexample.so.1
root> echo $?
1
```

如果缺少必需的库，在继续安装之前先安装该库。

**更多信息：**

rpm --requires－检测库依存关系 (p. 18)

# 修改安装之后 Oracle 数据库的主机设置

**症状：**

在安装企业管理服务器之后，我需要修改 Oracle 数据库服务器设置以指向不同的服务器。

**解决方案：**

您可以修改企业管理服务器，以便在安装之后与不同主机上的 Oracle 数据库一起使用：

1. 停止企业管理服务器上的 JBoss 应用程序服务器服务。
2. 备份当前主机上的 Oracle 数据库。
3. 还原新主机上的 Oracle 数据库。
4. 导航到以下目录，其中 *JBoss_HOME* 表示 JBoss 的安装目录：

   *JBoss_HOME*/server/default/deploy
5. 定位并备份下列文件：
   - imauditdb-ds.xml
   - imquartzdb-ds.xml
   - imtaskpersistencedb-ds.xml
   - imworkflowdb-ds.xml
   - objectstore-ds.xml
   - reportsnapshot-ds.xml
6. 打开每个文件，并找到 <connection-url> 条目。
7. 修改连接设置以便指定新的 Oracle 数据库主机名。例如：

   <connection-url>jdbc:oracle:thin@//*new_host_name*:1521/*sid_or_service_name*</connection-url>
8. 启动 JBoss 应用程序服务器服务。

   您已经修改 Oracle 数据库主机设置。

# 企业管理服务器无法注册端点类型

**症状：**

在安装企业管理服务器之后，在尝试注册端点时，无法查看端点类型。

**解决方案：**

componentregistration 实用程序 注册企业管理服务器端点。安装无法注册端点时，您可以手动运行 componentregistration 实用程序。

**遵循这些步骤:**

1. 登录到企业管理服务器。
2. 打开命令提示符窗口，并导航到以下 bin 目录：

   ```
   \ProgramFiles\CA\AccessControlServer\APMS\AccessControl\bin\
   ```

3. 通过运行以下命令执行 ComponentRegistration 实用程序：

   ```
   ComponentRegistration -comp jcs -register -userDN <user> -serverDN <server>
   -pwd <communication_password> -port CA Portal -ssl yes
   ```

   例如：ComponentRegistration -comp jcs -register
   -userDN cn=root,dc=etasa -serverDN dc=im,dc=etasa
   -pwd password -port 20411 -ssl yes

4. 重新启动 CA Access Control 服务。
5. 确认端点类型通过登录到 CA Access Control 企业管理进行注册。
6. 浏览“特权帐户”、“端点”、“查看端点类型”并检查列出的端点类型。

您已成功注册端点类型。

# CA Access Control 企业管理 安装期间出现“解释程序错误”错误消息

**在 UNIX 和 Linux 上有效**

**症状：**

我尝试安装 CA Access Control 企业管理 时，收到以下错误消息：

```
/bin/sh：解释程序错误：权限被拒绝
```

**解决方案：**

在某些 UNIX 或 Linux 发行版中，操作系统会使用 noexec 选项自动装入光盘驱动器。要安装 CA Access Control 企业管理，请确定未使用 noexec 选项挂接光盘驱动器。

# 无法在 CA Access Control 企业管理 数据库密码中使用 $ 字符

**症状：**

在安装 CA Access Control 企业管理 时，我输入数据库密码后收到以下错误消息：“无法检测到数据库版本”。

**解决方案：**

如果您在密码的结尾输入 $ 字符，CA Access Control 企业管理 安装会显示此错误消息。如果必须要在密码的结尾放置 $ 字符，必须在安装之后更改数据库密码。

# 无法打开 CA Access Control 服务器组件

**症状：**

在启动所有必备 CA Access Control 服务后，我无法在 Web 浏览器中打开 CA Access Control 企业管理、CA Access Control 端点管理 或 CA Access Control 密码管理器。我在同一服务器上安装了 JBoss 和 Oracle。

**解决方案：**

Oracle 和 JBoss 都使用默认端口 8080。要解决此问题，必须解决 Oracle 和 JBoss 之间的端口冲突。在更改 Oracle 或 JBoss 端口之前，您应考虑哪种更改更易于在您的企业中实施。

使用以下过程可更改默认的 JBoss 和 Oracle 端口：

### 更改默认 JBoss 端口

1. 打开命令窗口并导航到以下目录，其中 *JBossInstallDir* 是您安装 JBoss 的目录：

   *JBossInstallDir*/bin

2. 停止 JBoss：

   - (Windows) shutdown.bat -S
   - (UNIX) shutdown.sh -S

3. 在文本编辑器中打开以下文件：

   *JBossInstallDir*/server/default/deploy/jbossweb-tomcat55.sar/server.xml

4. 在以下部分中更改端口号：

   ```
   <!-- A HTTP/1.1 Connector on port 8080 -->
       <Connector port="8080" address="${jboss.bind.address}"
   ```

5. 保存并关闭文件。

6. 在文本编辑器中打开以下文件：

   *JBossInstallDir*/server/default/deploy/httpha-invoker.sar/META-INF/jboss-service.xml

7. 在下列各行中更改端口号：

   ```
   <attribute
   name="InvokerURLSuffix">:8080/invoker/EJBInvokerServlet</attribute>
   <attribute
   name="InvokerURLSuffix">:8080/invoker/EJBInvokerHAServlet</attribute>
   <attribute
   name="InvokerURLSuffix">:8080/invoker/JMXInvokerServlet</attribute>
   <attribute
   name="InvokerURLSuffix">:8080/invoker/readonly/JMXInvokerServlet</attribute>
   <attribute
   name="InvokerURLSuffix">:8080/invoker/JMXInvokerHAServlet</attribute>
   ```

8. 保存并关闭文件。

9. 启动 JBoss。

10. (Windows) 如下所述更改 CA Access Control 企业管理、CA Access Control 端点管理 和 CA Access Control 密码管理器快捷方式：

    a. 依次单击“开始”、“程序”、“CA Access Control”，然后右键单击相应的快捷方式。

       例如：要更改 CA Access Control 企业管理 快捷方式，请依次单击“开始”、“程序”、“CA Access Control”，然后右键单击“企业管理”。

    b. 单击“属性”。

    c. 将 URL 字段中的端口号更改为新的 JBoss 端口号。

**更改默认 Oracle 端口**

1. 启动 SQL 命令行。
2. 以 sysdba 身份连接到 Oracle：

   ```
   connect / as sysdba
   ```

3. 检查当前用于 HTTP 通讯的是什么端口：

   ```
   select dbms_xdb.gethttpport from dual;
   ```

4. 将端口设置为所需端口号：

   ```
   exec dbms_xdb.sethttpport('portNumber');
   ```

5. 停止并重新启动数据库。

   ```
   shutdown immediate
   ```
   启动

# CA Access Control 企业管理 中的选项卡不可见

**适用于 Active Directory 用户存储**

**症状：**

我已成功安装 CA Access Control 企业管理。当我以安装期间指定的系统用户身份登录时，界面中没有显示任何选项卡。

**解决方案：**

在安装 CA Access Control 企业管理 时，请提供下列 Active Directory 参数：

- 主机
- 端口
- 搜索根

- 用户 DN（以及此用户的密码）
- 系统用户

当 Active Directory 搜索根与用户 DN（可分辨名称）和系统用户的 DN 位于目录树的同一节点中时，会发生此问题。要解决此问题，请在目录树中指定搜索根比指定用户 DN 和系统用户的 DN 高一个或多个节点。

### 示例：Active Directory 搜索根

本示例为用户 DN 和系统用户使用以下 DN：

- 用户 DN：CN=MyQueryUser,OU=ENTERPRISE,OU=NFS, OU=ACCOUNTS,DC=EXAMPLE,DC=LAB
- 系统用户：CN=MySystemManager,OU=ENTERPRISE,OU=NFS, OU=ACCOUNTS,DC=EXAMPLE,DC=LAB

以下搜索根在目录树中比用户 DN 和系统用户的 DN 高一个节点。如果您指定以下搜索根，CA Access Control 企业管理 将成功安装并且界面中将显示选项卡：

```
OU=NFS,OU=ACCOUNTS,DC=EXAMPLE,DC=LAB
```

以下搜索根与用户 DN 和系统用户的 DN 位于目录树的同一节点中。如果您指定以下搜索根，CA Access Control 企业管理 将成功安装但界面中不会显示任何选项卡：

```
OU=ENTERPRISE,OU=NFS,OU=ACCOUNTS,DC=EXAMPLE,DC=LAB
```

### 示例：将 Active Directory 搜索根设置为目录树中高出一个节点

本示例为用户 DN 和系统用户使用的 DN 与前一示例相同：

在本示例中，您在安装 CA Access Control 企业管理 时指定了以下搜索根：

```
OU=ENTERPRISE,OU=NFS,OU=ACCOUNTS,DC=EXAMPLE,DC=LAB
```

因为此搜索根与用户 DN 和系统用户的 DN 位于目录树的同一节点中，所以您需要将搜索根指定为目录树中高出一个节点。

**将 Active Directory 搜索根设置为目录树中高出一个节点**

1. 启用 Identity Manager 管理控制台。
2. 打开 Identity Manager 管理控制台。
3. 单击“目录”，然后单击 ac-dir 目录。

   此时将显示“目录属性”对话框。
4. 单击“目录属性”对话框底部的“导出”。
5. 出现提示时，保存 XML 文件，然后打开以进行编辑。

   **注意：**文件名为 ac-dir.xml。

6. 找到包含您在安装期间指定的搜索根的标记。例如：

   ```
   <LDAP searchroot="OU=ENTERPRISE,OU=NFS,OU=ACCOUNTS,DC=EXAMPLE,DC=LAB"
   secure="false"/>
   ```

7. 将现有搜索根替换为新的搜索根。例如：

   ```
   <LDAP searchroot="OU=NFS,OU=ACCOUNTS,DC=EXAMPLE,DC=LAB" secure="false"/>
   ```

   **注意：**因为您已删除企业 OU（组织单元），所以此搜索根在目录树中比前一搜索根高一个节点。

8. 保存并关闭文件。

9. 在 Identity Manager 管理控制台中，单击“目录属性”对话框中的“更新”。

   此时将显示“更新目录”页面。

10. 单击“选择文件”，导航到您编辑过的 XML 文件，单击“打开”，然后单击“完成”。

    Identity Manager 管理控制台会验证 XML 文件，并在“目录配置输出”字段中显示状态信息。

    **注意：**如果您收到“无法导入”错误，请参阅“无法导入 ac-dir.xml 目录配置文件”主题。

11. 单击“继续”。

    此时将显示“目录”页面。

12. 单击 ac-dir，然后单击“环境”部分中的 ac-env。

    此时将显示“环境属性”页面。

13. 单击“重新启动”。

    Identity Manager 管理控制台将重新启动环境并应用您所做的更改。

**注意：**有关如何启用和启动 Identity Manager 管理控制台的详细信息，请参阅 *《实施指南》*。

# 无法导入 ac-dir.xml 目录配置文件

**症状：**

我从 Identity Manager 管理控制台导出了 ac-dir.xml 目录配置文件。我试图导入该文件时，“目录配置输出”字段中显示以下错误消息：

```
正在部署目录配置...

正在分析输入流...
错误：(140:67)：cvc-complex-type.4：属性“value”必须出现在元素“容器”上。
错误：无法导入

*********
1 个错误，0 个警告
```

**解决方案：**

ac-dir.xml 目录配置文件描述了用户存储的结构和内容。可使用此文件来更改 CA Access Control 企业管理 如何与用户存储交互，例如：更改用户目录密码或 Active Directory 搜索根。还可在针对 SSL 通讯配置 CA Access Control 企业管理 以及针对故障转移配置 Active Directory 时编辑 ac-dir.xml 文件。

要解决此问题，请执行以下操作：

1. 打开 ac-dir.xml 文件进行编辑。
2. 找到以下标记：

   ```
   <Container objectclass="top,organizationalUnit" attribute="ou"/>
   ```

3. 将以前的标记替换为以下标记：

   ```
   <Container objectclass="top,organizationalUnit" attribute="ou" value=""/>
   ```

4. 保存并关闭文件。

现在，您可以将目录配置文件导入到 Identity Manager 管理控制台中。要应用您在目录配置文件中所做的更改，必须在导入文件后重新启动环境。

# CA Access Control 企业管理 无法连接到 DMS

**症状：**

我在登录到 CA Access Control 企业管理 时，收到类似如下的消息：

```
错误：登录过程失败
错误：目标上的密码与客户端的密码不符
```

**解决方案：**

用户 ac_entm_pers 无法登录到 DMS。此用户会对企业管理服务器和 DMS 之间的通讯和数据流进行身份验证。

**注意：**ac_entm_pers 用户具有以下授权属性：ADMIN、AUDITOR、IGN_HOL、LOGICAL

要排除此问题，请执行以下操作：

1. 打开 selang。
2. 连接到 DMS：

   ```
   host DMS__@entM_host_name
   ```

3. 更改 ac_entm_pers 的密码：

   ```
   eu ac_entm_pers admin auditor nonative password(password) logical nonative grace-
   ```

4. 授权 ac_entm_pers 可登录到安装了企业管理服务器的主机：

   ```
   authorize TERMINAL entM_host_name uid(ac_entm_pers) access(a)
   ```

5. 验证 ac_entm_pers 是否可以登录到企业管理服务器：

   ```
   host DMS_@entM_host_name uid(ac_entm_pers) password(password) logical
   ```

6. 使用 ac_entm_pers 的新密码更新企业管理服务器 DMS 连接设置。

   DMS 会对 ac_entm_pers 进行身份验证，CA Access Control 企业管理将连接到 DMS。

   **注意：**有关如何配置与 DMS 的连接的详细信息，请参阅 *CA Access Control 企业管理 联机帮助*。

如果您在更新连接设置时收到错误，DMS 将无法对 ac_entm_pers 进行身份验证。要排除此问题，请执行以下操作：

1. 确定您在前面过程的每个步骤中输入了相同的密码。
2. 确定前面过程步骤 4 中的企业管理服务器主机名 (*entM_host_name*) 是正确的。

   例如：如果您在步骤 4 中指定了企业管理服务器的完全限定主机名，但企业管理服务器的 TERMINAL 记录使用短主机名，则不会解析主机名且 ac_entm_pers 无法登录到企业管理服务器。

3. 查看 CA Access Control 审核文件：

   ```
   seaudit -a
   ```

4. 查看 DMS 审核文件：

   ```
   seaudit -a -fn DMS_log_file
   ```

   **注意：**审核记录可能会提供有关企业管理服务器的 TERMINAL 记录中的正确主机名的信息。

### 示例：显示 DMS 审核文件

以下示例显示了名为 DMS__ 的 DMS 审核文件：

```
seaudit -a -fn "C:\Program
Files\CA\AccessControlServer\APMS\AccessControl\Data\DMS__\pmd.audit"
```

## CA Access Control 企业管理 选项卡中显示问号

**症状：**

我在打开 CA Access Control 企业管理 时，看到选项卡中显示问号。

**解决方案：**

要解决此问题，请将您浏览器的默认语言更改为“英语 (美国)”。

## 在 InfoView 中收到的“空页面”错误

**症状：**

我试图访问 CA Access Control 报告时，在 InfoView 中出现以下错误：

空页面：无法从报告源创建页面

**解决方案：**

在 Windows 上，可能是未正确定义或安装 CA Access Control Universe。测试 CA Access Control Universe 的连接。如果连接不正常，请编辑连接；如果连接正常，请替换连接。

在 Solaris 上，以 bouser 身份登录并按以下所述编辑脚本 $CASHCOMP/CommonReporting/bobje/setup/env.sh：

1. 附加以下 LIBRARYPATH：

   ```
   $MWHOME/lib-sunos5_optimized
   ```

2. 重新启动 BusinessObjects 服务：

   ```
   cd $CASHCOMP/CommonReporting/bobje
   ./stopservers
   ./startservers
   ```

# CA Access Control 在 UNIX 上安装后不自动启动

**在 UNIX 上有效**

**症状：**

在我将 CA Access Control 安装在 UNIX 端点上之后，CA Access Control 没有自动启动。

**解决方案：**

默认情况下，CA Access Control 不会在 UNIX 端点上自动启动。

要将 seosd 后台进程配置为在 UNIX 计算机启动时自动启动，请使用 *ACInstallDir*/samples/system.init/*sub-dir* 目录，其中 *sub-dir* 是您操作系统的目录。每个子目录都包含一个自述文件，其中包含有关如何在您的操作系统上自动启动 CA Access Control 的说明。

**注意：**有关如何启动 CA Access Control 的详细信息，请参阅*《实施指南》*。

# 无法在 Linux s390 端点上启动后台进程

**在 Linux s390 和 Linux s390x 上有效**

**症状：**

我无法启动 seosd 或 ReportAgent 后台进程。

**解决方案：**

CA Access Control 无法在端点上找到 Java 环境。要解决此问题，请执行以下操作：

1. 确定 accommon.ini 文件 global 部分中的 java_home 配置设置包含 Java 环境的路径。
2. 将 LD_LIBRARY_PATH 环境变量的值设置为 Java 环境的共享库的路径。

# 安装后无法连接到 selang

**症状：**

我在安装 CA Access Control 之后尝试启动 selang 或连接到 CA Access Control 数据库时，收到以下错误：

```
错误：初始化失败，正在退出!
(localhost)
错误：登录过程失败
错误：不允许从终端 example.com 管理此站点
```

**解决方案：**

没有正确定义终端规则。请排除终端规则故障以确定问题原因。

**排除终端规则故障**

1. 停止 CA Access Control：

   ```
   secons -s
   ```

2. 以本地模式启动 selang：

   ```
   selang -l
   ```

   **注意：**只有 root 用户可以在 UNIX 计算机上以本地模式运行 selang。

3. 检查您是否已为本地终端 (*terminal_name*) 创建 TERMINAL 记录，以及是否已正确定义终端访问权限：

   ```
   showres TERMINAL terminal_name
   ```

   - 如果记录不存在，请为本地终端创建 TERMINAL 记录：

     ```
     editres TERMINAL terminal_name owner(name) defaccess(accessAuthority)
     ```

     **注意：**所有者可以是一个用户，也可以是一个组。因为 TERMINAL 记录的默认访问权限为 none，建议您在创建记录时指定默认访问权限，以免用户被锁定在终端之外。

   - 如果终端访问权限不正确，请为终端定义正确的访问权限：

     ```
     authorize TERMINAL terminal_name uid(name) access(accessType)
     ```

4. (UNIX) 检查 [seosd] 部分中 terminal_default_ignore 配置设置的值。

   此配置设置用于确定在授予管理访问权限时 CA Access Control 是否考虑 _default TERMINAL 和具体 TERMINAL 记录的 defaccess 值。

   **注意：**有关 terminal_default_ignore 配置设置的详细信息，请参阅*《参考指南》*。

5. (UNIX) 检查后备数据库是否反映终端，如下所示：
   a. 构建特定于主机名的后备数据库：

      ```
      sebuilda -h
      ```

   b. 检查后备数据库中的终端入口和主机名是否相同：

      ```
      sebuilda -H | grep hostname
      ```

      将列出主机后备数据库文件的内容。
6. 启动 CA Access Control：
   - (UNIX) seload
   - (Windows) seosd -start

**注意：**如果仍无法启动 selang 或连接到 CA Access Control 数据库，您可能需要修改操作系统的 hosts 文件。请联系您的系统管理员或网络管理员以获取帮助。

# 显示在 Solaris 10 日志文件中的消息

**在 Solaris 10 上有效**

**症状：**

当我使用“secons -s”停止 CA Access Control 时，CA Access Control 消息显示在我的 Solaris 10 计算机上的“/var/adm/messages”日志文件中。我计算机上的 SEOS_use_streams 配置设置已设为 yes。

**解决方案：**

这些消息仅为提供信息之用，不表明任何失败或错误。您无需进行任何操作。消息及其解释如下：

- “SEOS: Restored tcp wput” “SEOS: Restored strrhead rput”

  这些消息表明 SEOS_syscall 功能禁用了网络 hook。
- “SEOS: Replaced tcp wput” “SEOS: Replaced strrhead rput”

  这些消息表明 SEOS_syscall 功能启用了网络 hook。

# 在卸载期间手动删除注册表键时收到错误

**在 Windows 上有效**

**症状：**

在卸载 CA Access Control 期间，当我尝试删除注册表键时，收到以下错误消息：

无法打开数据：打开注册表键时出错。

**解决方案：**

运行 RemoveAC.exe 实用程序以删除 CA Access Control 注册表键和目录。RemoveAC.exe 实用程序不会卸载产品，但可帮助确保从计算机中删除所有 CA Access Control 注册表键和目录。

# ProductExplorer 未启动

**症状：**

当我将适用于 Windows 的 CA Access Control Server Components DVD 插入光盘驱动器时，ProductExplorer 没有启动。

**解决方案：**

请执行以下操作：

- 请导航至光盘驱动器目录并双击 ProductExplorerx86.EXE 文件。
- 启用 autorun 以自动启动 ProductExplorer。

# 升级到 CA Licensing 1.9.04 时发生许可错误

**在 UNIX 上有效**

**症状：**

升级 CA Access Control 时，新的 CA Licensing rpm 脚本 (1.9.04) 首先执行。然后，先前 rpm 脚本的卸载程序执行，且在 UNIX syslog 中记录以下错误消息：

```
<Error opening lic98.err - /opt/CA/SharedComponents/ca_lic/lic98.err, original
code=5000>2E2U eTrust Access Control for UNIX <Error opening lic98.err -
/opt/CA/SharedComponents/ca_lic/lic98.err, original code=5000>  LRF=2E2U,
000000000000, Linux_x86.64_1_*, ismelx84, 0
```

**解决方案：**

CA Licensing 1.9.03 或更低版本的安装程序删除产生错误的链接和文件夹。我们建议您不要执行升级，但可直接安装 CA Licensing 版本 1.9.04。

**遵循这些步骤:**

1. 如果 CA Access Control 正在运行，通过以管理员身份登录并输入以下命令将其关闭：

   ```
   ACInstallDir/bin/secons -sk
   ACInstallDir/bin/SEOS_load -u
   ```

2. 将以下文件备份到临时文件夹：
   - /etc/profile.
   - /etc/profile.CA.
   - /etc/csh_login.CA.
   - 请注意以下条目的所有符号链接信息：
     - /usr/local/CAlib
     - /opt/CA/CAlib
     - $CASHCOMP/CAlib
     - /ca_lic
     - /opt/CA/ca_lic
     - $CASHCOMP/ca_lic
     - $CASHCOMP/lib
3. 备份所有符号目录。
4. 从支持网站下载最新的 CA Licensing 数据包。
5. 将压缩文件的内容提取到临时目录。

6. 导航到新的 lic98_install 目录。
7. 输入以下命令安装 CA Licensing：

   ```
   ./install <install directory>
   ```

8. 输入以下命令获取 /etc/profile：

   ```
   ./etc/profile
   ```

9. 执行下列步骤还原 ca.olf 文件：

   a. 运行以下命令：

      ```
      rpm -e --nodeps ca-lic
      ```

   b. 将在第 2 步中备份的目录还原到以下目录：

      ```
      /opt/CA/SharedComponents/ca_lic
      ```

   c. 将在第 2(d) 步中记下的符号链接还原到以下目录：

      ```
      /opt/CA/SharedComponents/ca_lic
      ```

   d. 将备份的 /etc/profile、/etc/profile.CA 和 /etc/csh_login.CA 文件还原到以下目录：

      ```
      /opt/CA/SharedComponents/ca_lic
      ```

   CA Licensing 1.9.04 即成功安装，您可以继续使用所有注册过的 CA 产品。

# 在企业管理服务器上阻止 HTTP 访问

**症状：**

安装之后，HTTP 和 HTTPS 端口在默认情况下是开放的。您需要禁用 HTTP 端口。

**解决方案：**

为了禁用 HTTP 端口，在 JBoss 配置中注释掉 HTTP 连接器。

**遵循这些步骤:**

1. 浏览到 *JBOSS_HOME*/server/default/deploy/jboss-web.deployer 并编辑 server.xml 文件。
2. 搜索以下字符串，这些字符串定义 HTTP 连接器的默认端口：_
   `port="18080"`

   **注意：**如果您已在安装向导中配置了其他端口，那么端口号可能有所不同。

   此端口属性是 <Connector> 元素的一部分。
3. 通过使用注释标记(<!-- _ 和 -->)环绕元素来注释掉此 <Connector> 元素。

   HTTP 连接器已禁用。
4. 重新启动 JBoss 服务。

## 示例

```
<!-- <Connector port="18080" address="${jboss.bind.address}"
         connectionTimeout="20000" /> -->
```

# 第 3 章： 创建策略和访问权限

此部分包含以下主题：



## 拦截用户访问网络驱动器和共享驱动器

**在 Windows 上有效**

**症状：**

我可以拦截用户访问系统驱动器，但我无法停止用户访问网络和共享驱动器。

**解决方案：**

要在 Windows 2008 上拦截用户访问网络和共享驱动器，请将以下 selang 命令添加到策略中：

```
newres FILE \Device\Mup\*
```

要在 Windows 2003 上拦截用户访问网络和共享驱动器，请将以下 selang 命令添加到策略中：

```
newres FILE \Device\LanmanRedirector\*
```

# 用户可以访问受保护的资源

**症状：**

我为资源创建了默认访问权限 none，但超级用户仍可访问该资源。

**解决方案：**

排除资源访问问题 (p. 114)。

# 读取访问权限检查跳过 /etc/passwd 和 /etc/group 文件

**在 UNIX 上有效**

**症状：**

我创建了一个 /etc/passwd 和 /etc/group 文件的默认访问权限为 none 的规则，但我对这些文件仍有读取访问权限。

**解决方案：**

默认情况下，CA Access Control 授权引擎会跳过对 /etc/passwd 和 /etc/group 系统文件的读取访问权限检查。要使 CA Access Control 停止跳过对系统文件的读取访问权限检查，请将 seos.ini 文件 [seosd] 部分中的 bypass_system_files 的值更改为 no。

**重要说明！** 如果使 CA Access Control 停止跳过对系统文件的读取访问权限检查，请确定是否设置了正确的授权。如果未设置正确的授权却跳过读取访问权限检查，包括 CA Access Control 管理员和 root 用户在内的用户可能无法访问系统，关键的系统进程可能失败。

# 企业用户或组不能访问资源但可以设置正确的访问规则

**在 Windows 上有效**

**症状：**

我看到企业用户或组具有访问资源的权限，但他们却不能访问资源。

**解决方案：**

企业帐户可能已被循环使用，数据库中的权限适用于旧帐户而不适用于名称相同但 SID 不同的新帐户。要检查此情况，请解析循环企业帐户。

**注意：**有关解析循环企业帐户的详细信息，请参阅*《适用于 Windows 的端点管理指南》*。

# 登录失败时不锁定用户

**在 UNIX 上有效**

**症状：**

我将 serevu 配置为当失败的登录尝试次数达到指定数值后在密码 PMD 中禁用用户。在用户无法正确登录时，CA Access Control 不锁定该用户。在我使用 nodaemon 选项启动 serevu 以查看 pam_failed_logins.log 文件时，服务器未响应。

**解决方案：**

seos.ini 文件 [seos] 部分中的 passwd_pmd 的值不正确。将 passwd_pmd 的值设置为 sepass 向其发送密码更新项的密码 PMD 的名称。

# 用户可在超出时间限制后运行命令

**症状：**

我为组设置了时间限制，但组成员在超出允许的时间后仍然可以运行 CA Access Control 命令。

**解决方案：**

在受限的时间段内，CA Access Control 可阻止用户启动新的登录对话，但无法强制用户断开连接。要阻止用户在受限的时间段内访问资源或命令，请更改资源或命令的资源记录以包括时间限制。

**注意：**CA Access Control 会先检查用户的 USER 或 XUSER 记录中是否存在时间限制，然后再检查该用户所属的 GROUP 或 XGROUP 是否存在时间限制。

# CA Access Control 将所有用户均识别为 root 用户

**在 UNIX 上有效**

**症状：**

在我以非 root 用户身份运行 sewhoami 实用程序时，CA Access Control 将该用户识别为 root 用户。

**解决方案：**

要排除此问题，请在登录应用程序的 LOGINAPPL 记录中确定以下内容：

- LOGINAPPL 记录的名称是登录应用程序的名称。
- LOGINAPPL 记录中的 LOGINPATH 参数指定了登录应用程序的正确完整路径。

  要确定登录应用程序的路径，请先运行跟踪 (p. 116)，然后使用登录应用程序登录和注销 CA Access Control。查看跟踪可获取路径。
- LOGINAPPL 记录中的 LOGINSEQUENCE 参数指定了登录应用程序的正确登录顺序。要获得帮助，请通过 http://ca.com/worldwide 与技术支持联系。

**注意：**CA Access Control 不会定义第三方登录应用程序的 LOGINAPPL 记录。如果您使用的是第三方登录应用程序，请手动定义该应用程序的 LOGINAPPL 记录。

# 无法将用户作为密码管理员仅添加到一个组

**症状：**

我想使得某个用户成为特定组的密码管理员，但在我执行以下命令时，该用户成为了所有组的密码管理员：

```
editusr userName pwmanager
```

**解决方案：**

如下所述指定要将用户作为密码管理员所添加到的组的名称：

```
join userName group(groupName) pwmanager
```

# Windows 管理员可以更改 CA Access Control 密码

**在 Windows 上有效**

**症状：**

Windows 管理员可以在受 CA Access Control 保护的 Windows 环境中更改 CA Access Control 密码。

**解决方案：**

要帮助确保只有 CA Access Control 中指定的用户才可以更改 CA Access Control 密码，请在以下注册表键中将 EnforceViaeTrust 注册表项的值设置为 1：

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\passwd
```

此注册表项指定实施只能通过 CA Access Control 更新或创建用户密码。该注册表项的默认值为 0，这意味着您不必使用 CA Access Control 来更新或更改用户密码。

# 全局密码策略将用户锁定在受保护的系统之外

**症状：**

在我实施全局密码策略时，该密码策略将用户锁定在受 CA Access Control 保护的系统之外。

**解决方案：**

为必须访问受 CA Access Control 保护的系统的用户创建一个单独的密码策略。可使用配置文件组为这些用户创建密码策略。

以下过程介绍了如何使用配置文件组实施密码策略：

1. 创建配置文件组。
2. 为配置文件组设置密码策略。
3. 将用户分配到该配置文件组。

   您为该配置文件组设置的密码策略现将适用于与该配置文件组关联的用户。

# 任务指派因交互式应用程序而挂起

**在 Windows 上有效**

**症状：**

我编写了一个任务指派规则，允许用户运行交互式 Windows 应用程序（例如：notepad.exe）。在用户尝试运行该应用程序时，任务指派挂起。

**解决方案：**

必须为允许用户运行应用程序的 SUDO 类记录设置交互式标志。如果您使用任务指派来运行交互式 Windows 应用程序但未设置交互式标志，则该应用程序将在后台运行，您无法与之交互。

要解决此问题，请执行以下操作：

1. 为 SUDO 记录设置交互式标志：

   `er SUDO resourceName interactive`

   ***resourceName***

   指定允许用户运行应用程序的资源记录的名称。

   现在为指定资源设置了交互式标志。

2. 如下所述重新启动任务指派服务：

   a. 终止交互式应用程序。

   b. 如果任务指派仍然挂起，请重新启动 CA Access Control。

**注意：**有关任务指派以及定义 SUDO 记录的更多信息，请参阅*《适用于 Windows 的端点管理指南》*。

# 第 4 章： 管理 CA Access Control 数据库

此部分包含以下主题：



## selang 查询最多返回 100 条记录

**症状：**

我运行应返回 100 条以上记录的 selang 查询时，CA Access Control 显示以下消息：

警告：仅显示 100（查询大小限制）项。

**解决方案：**

query_size 配置设置的默认值为 100。要增加 CA Access Control 为 selang 查询返回的记录数，请更改 query_size 配置设置的值。

query_size 配置设置位于：

- (UNIX) seos.ini 文件的 [lang] 部分
- (Windows) lang 子键，如下所示：

  HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\lang

# 备份数据库之后审核日志中出现 UTimes 和拒绝记录

**症状：**

我在 CA Access Control 正在运行的情况下使用操作系统备份工具备份 CA Access Control 数据库时，CA Access Control 向审核日志中发送了类似于以下消息的条目：

```
03 Mar 2008 15:58:01 D FILE            UTimes     69 10
/opt/CA/AccessControl/seosdb/seos_pvf.fre /usr/sbin/fbackup
```

**注意：**上述示例是使用 UNIX 路径名编写的，但解决方案同样适用于 Windows 计算机。

**解决方案：**

该审核消息表示 CA Access Control 阻止了备份操作更新 UTimes 文件日期戳。CA Access Control 没有阻止备份本身。

要防止此消息出现在审核日志中，请执行以下操作：

- 如果备份程序是由非超级用户执行的，请验证该用户是否具有 OPERATOR 属性。
- 如果备份程序是由超级用户执行的，请验证备份程序是否具有带有 pgmtype（备份）属性的 SPECIALPGM 记录。

要确保正确备份数据库，请使用 dbmgr 实用程序执行备份。

# CA Access Control 数据库损坏

**在 UNIX 上有效**

**症状：**

我在 CA Access Control 错误日志中发现类似如下的消息：

```
seoswd: [ID 973226 auth.error] 与 seosd 的通讯超时。正在执行 seosd
致命错误!
Inseosrt_InitDatabase (0x270)
警告: /Access Control 路径/seosdb/seos_cdf.dat 已损坏
```

**解决方案：**

使用以下过程可修复数据库损坏。

**注意：**此过程假定数据库安装在默认位置 /opt/CA/AccessControl/ 中。

### 修复 CA Access Control 数据库损坏

1. 停止 CA Access Control：

   ```
   secons -s
   ```

2. （可选）将数据库备份到其他位置，以便在需要时将数据库提供给技术支持。

3. 验证数据库是否标记为已关闭：

   ```
   cd /opt/CA/AccessControl//seosdb
   ```

   ```
   dbmgr -util -close
   ```

   **注意：**如果 CA Access Control 未正确关闭，数据库可能会标记为打开。

4. 检查数据库：

   ```
   dbmgr -util -check
   ```

5. 请执行下列操作之一：

   - 如果在检查数据库时没有收到错误消息，请转到步骤 6。
   - 如果在检查数据库时收到错误消息，则不要完成步骤 6 和 7；而是重建数据库 (p. 119)。

6. 构建数据库文件：

   ```
   dbmgr -util -build all
   ```

7. 再次检查数据库：

   ```
   dbmgr -util -check
   ```

8. 启动 CA Access Control：

   ```
   seload
   ```

**注意：**如果数据库仍是损坏的，则需要进一步调查。要获得帮助，请通过 http://ca.com/worldwide 与技术支持联系。

# 第 5 章： 连接到远程计算机

此部分包含以下主题：



## 无法连接到远程计算机

**症状：**

我无法连接到远程 CA Access Control 计算机。

**解决方案：**

排除连接问题 (p. 114)。

## syslog 中持续显示与 seosd 的通讯超时

**在 Windows 上有效**

**症状：**

在运行 CA Access Control 时，计算机有时运行缓慢且 syslog 中显示以下消息：

```
seoswd: 与 seosd 的通讯超时。正在执行 seosd
seoswd: 与 seosd 的通讯问题返回了 5378 [成功]
seoswd: 说明: 与 seosd 的通讯超时。
```

**解决方案：**

计算机上的防病毒软件导致 CA Access Control 超时。在防病毒软件中执行以下操作：

- 将 CA Access Control 目录从实时扫描中排除
- 停止对 CA Access Control 目录的实时（访问时）扫描

因为 CA Access Control 在默认情况下保护 CA Access Control 注册表键、文件和安装目录，所以之前的操作不会增加对计算机的病毒威胁。

建议您为防病毒软件创建一条 SPECIALPGM 记录，并将该 SPECIALPGM 记录的 PGMTYPE 属性设置为 pbf。pbf 程序类型会跳过对文件处理事件的数据库检查。

# 无法控制第一个传入 ftp 连接

**在 UNIX 上有效**

**症状：**

当我启动 CA Access Control 时，它无法控制来自 vsftpd 的第一个传入 ftp 连接。我已经创建了 ftp 的 TCP 规则和 vsftpd 的 HOST 规则，CA Access Control 会根据我创建的 TCP 或 HOST 规则控制来自 vsftpd 的所有后续传入 ftp 连接。

**解决方案：**

如果您在启动 CA Access Control 之前启动了 vsftpd，vsftpd 会在接受系统调用中为传入 ftp 连接放置一个挂钩。该挂钩意味着在 vsftpd 处理第一个传入 ftp 连接之后 CA Access Control 才能截获连接。

vsftpd 在处理该 ftp 连接之后，会尝试调用接受系统调用以准备处理下一个 ftp 连接。但是，CA Access Control 将截获此系统调用并因此控制所有后续 ftp 连接。

要截获第一个传入 ftp 连接，请使用下列变通方法之一：

- 在启动 vsftp 之前启动 CA Access Control。
- 使用超级服务器后台进程（如 inetd 或 xinetd）启动 vsftpd。

  **注意：**有关配置超级服务器后台进程的详细信息，请与您的操作系统供应商联系。
- 在启动 CA Access Control 后运行 tripAccept 实用程序。

  要运行 tripAccept 实用程序，必须启用 seos.ini 文件 [SEOS_syscall] 部分中的 call_tripAccept_from_seload 标记。建议您在运行 tripAccept 实用程序之前先为其定义一条 SPECIALPGM 记录。

# 本地主机和目标主机上的目标页面不同

**在 UNIX 上有效**

**症状：**

我尝试连接到 CA Access Control 主机时，出现以下消息：

警告：本地计算机与目标主机的代码页不同。

**解决方案：**

验证 seos.ini 文件 [seos] 部分中的 locale 配置设置在本地主机和目标主机上的值是否相同。

# 无法使用 selang 连接到端点

**症状：**

我尝试使用 selang 连接到端点时，收到类似如下的错误消息：

数据解包失败

**解决方案：**

用于保护组件间通讯的加密存在问题。检查 CA Access Control 计算机中最近对加密密钥和加密方法所做的更改。

**注意：**有关加密方法的详细信息，请参阅 *《实施指南》*。

# 第 6 章： 从 PMD 部署规则

此部分包含以下主题：



## 订户 PMDB 无法从主 PMDB 接收更新

**症状：**

我有一个分层的 PMDB 体系结构。订户 PMDB 没有从主 PMDB 接收到更新。主 PMDB 的错误日志中包含以下消息：

无法接收来自非父 PMDB 的更新

**解决方案：**

如果订户 PMDB 没有从主 PMDB 接收到更新，请使用以下过程排除该问题。

**排除 PMDB 更新问题**

1. 列出主 PMDB 的订户 (*master_pmdb_name*) 及其状态：

   `sepmd -L master_pmdb_name`

   **注意：**在主 PMDB 计算机上运行此命令。

2. 查看订户列表以确定哪些订户不可用。

3. 验证每个不可用订户的 parent_pmd 配置设置的值是否正确。

   parent_pmd 配置设置位于：

   - (UNIX) seos.ini 和 pmd.ini 文件的 [seos] 部分
   - (Windows) 以下注册表键：

     `HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\AccessControl`

   **注意：**您在 parent_pmd 标记中指定的主机名必须与主 PMDB 的主机名完全匹配。验证是否已正确配置主机名解析可能有助于排除此问题。如果您使用的是 UNIX 计算机，可以使用 sehostinf 实用程序来发现主 PMDB 的主机名。要获得帮助，请通过 http://ca.com/worldwide 与技术支持联系。

如果问题仍然存在，请执行以下操作：

1. 显示主 PMDB 错误日志：

   ```
   sepmd -e master_pmdb_name
   ```

2. 查看错误日志，并注意针对不可用订户报告了哪些错误代码。
3. 对于每个不可用订户，使用错误代码来排除该问题。

如果问题仍然存在，请执行以下操作：

1. 从主 PMDB 所维护的不可用订户列表中删除问题订户：

   ```
   sepmd -r pmdb_name subscriber_name
   ```

   父 PMDB 会尝试将更新发送到订户。

2. 重复前面的过程。
3. 如果订户列表或父 PMDB 错误日志发生了任何更改，请使用这些更改来排除问题。

# 订户端点审核日志中出现失败事件

**症状：**

订户没有从主 PMDB 接收到更新。我在订户的 CA Access Control 审核日志中发现了*失败*事件。

**解决方案：**

PMDB 用户不具有 ADMIN 属性。要为 PMDB 用户提供 ADMIN 属性，请使用以下 selang 命令编辑用户记录：

```
chusr userName admin
```

**注意：**您必须具有 ADMIN 属性才能运行此 selang 命令。CA Access Control 会在将 PMDB 更新部署到订户时跳过 TERMINAL 规则。

# 第 7 章： 部署策略

此部分包含以下主题：



## 排除策略部署故障

将策略分配给主机时，只有 policyfetcher 检索部署任务并运行策略脚本之后，才会在分配的端点上部署该策略。因此，在端点上传输或部署策略时，可能会由于多种原因而导致部署错误。

为了解决策略部署错误，高级策略管理为您提供了一些故障排除操作。您可以使用 CA Access Control 企业管理 或 policydeploy 实用程序执行这些操作。在 CA Access Control 企业管理 中，故障排除操作位于“策略管理”选项卡的“策略”子选项卡中。

故障排除操作如下所述：

- **重新部署**－创建包含策略脚本的一项新部署任务并将该任务部署到端点。

  在端点上部署策略出现错误时可使用该选项。即，selang 策略脚本执行失败。需要先手动解决端点上脚本错误的原因，才能重新部署策略。

  **注意：**该选项仅在 CA Access Control 企业管理 中提供，在 policydeploy 实用程序中不受支持。

- **取消部署**－从指定端点取消部署策略，但不从相应主机取消分配该策略。

  使用该选项可从端点中删除未分配给 DMS 上的主机的任何策略。

- **重置**－重置端点。CA Access Control 可重置主机状态、取消部署所有有效策略，以及删除所有 GPOLICY、POLICY 和 RULESET 对象。

  使用该选项可从所有策略部署清除端点及其在 DMS 上的状态。

  **注意：**该选项不会从端点或 DMS 中删除 DEPLOYMENT 或 GDEPLOYMENT 对象，因为您可能需要使用这些对象来进行审核。在重置端点之后，可使用 dmsmgr -cleanup 功能删除 DEPLOYMENT 对象和 GDEPLOYMENT 对象。在重置端点之后，可以照常将策略分配给该端点。

- **还原**－在指定主机上取消部署任何策略，然后还原应该在主机上部署（分配或直接部署）的所有策略，方法是创建新部署任务并将这些任务发送到主机执行。

  当您在端点上重新安装 CA Access Control 或操作系统时，或者当您从备份还原端点时，可使用该选项来重新部署 DMS 指示在该端点上有效的所有策略。

# 策略未在所有端点上成功部署

**症状：**

我将某个策略部署到了主机组。策略在主机组中的有些主机上已成功部署，但在有些主机上部署时出错。

**解决方案：**

要解决此问题，请执行以下操作之一：

- 如果策略在少数主机上失败，请在这些主机上重新部署策略。

  您需要先手动解决主机上部署错误的原因，才能重新部署策略。

- 如果策略在许多主机上失败，则需要在每个端点上运行 policydeploy -fix 函数。

  policydeploy -fix 函数会修复并重新部署指定的部署任务或部署程序包。使用此函数时需要部署任务的名称。

**注意：**有关 policydeploy 实用程序的详细信息，请参阅*《参考指南》*。

### 示例：policydeploy -fix 函数

以下示例可修复端点上的指定部署程序包：

```
policydeploy -fix -task 1266471565#0f6a3cec-a37d-47d9-bde3-0112a49b714a
```

# DH 或灾难恢复 DMS 无法重新订阅

**症状：**

作为灾难恢复过程的一部分，我为 DH 重新订阅 DMS，或为灾难恢复 DMS 重新订阅生产 DMS。此时出现以下消息：

无法在 *dms@host* 上为 *subscriber* 重新订阅。
要完成还原操作，请通过指定偏移 *value* 在 *dms@host* 上为 *subscriber@host* 重新订阅。

**解决方案：**

如果为 DH 或灾难恢复 DMS 重新订阅的父 DMS 未运行，将出现该消息。您必须使用消息中的偏移值为 DH 手动重新订阅 DMS，或者为灾难恢复 DMS 手动重新订阅生产 DMS。指定偏移值可确保订户仅发送还原其数据库时未存在于数据库中的命令。

要为 DH 或灾难恢复 DMS 重新订阅其父 DMS，请在父 DMS 主机上运行以下命令：

```
sepmd -s parent_name child_name@host offset
```

### 示例：为 DH 订阅 DMS

以下示例使用偏移值 18028 为 DH__@test.com 订阅 DMS__。在 DMS__ 上运行以下命令：

```
sepmd -s DMS__ DH__@test.com 18028
```

# 策略状态为“未执行”

**症状：**

我已启用策略验证。在我部署策略时，策略未部署，且策略状态为“未执行”。

**解决方案：**

策略验证在策略中发现一个或多个错误。您必须先修复这些错误，然后才能成功部署策略。

要成功部署策略，请执行下列步骤：

1. 查看错误。

   您必须先确认错误是发生在策略中还是发生在 CA Access Control 数据库中，然后才能进行修复。

   a. 在 CA Access Control 企业管理 中，单击“策略管理”，再单击“策略”子选项卡，在左侧的任务菜单中展开“部署”树，然后单击“部署审核”。

      将显示“部署审核”页面。

   b. 定义搜索范围，然后单击“执行”。

      将显示与定义的搜索范围匹配的部署任务列表。

   c. 单击未部署的部署任务名称。

      将显示有关部署的信息，包括策略中的错误列表。

2. （可选）如果错误发生在 CA Access Control 数据库中，请执行以下操作：

   a. 修复 CA Access Control 数据库中的错误。

   b. 请执行下列操作之一：

      - 使用 policydeploy 实用程序修复部署任务。

        修复部署任务将删除部署任务的“失败”状态，如果部署成功，会将端点上的策略状态更改为“已部署”。

      - 使用 CA Access Control 企业管理 或 policydeploy 实用程序再次部署策略。

        再次部署策略会创建另一个部署任务。出错的上一个部署任务的状态仍然为“失败”状态。如果部署成功，端点上的策略状态为“已部署”。

3. （可选）如果错误发生在策略中，请执行以下操作：

   a. 创建一个不包含错误的新策略版本。

   b. 使用 CA Access Control 企业管理 或 policydeploy 实用程序升级策略。

# 策略状态为“已取消部署，但存在失败”

**症状：**

在尝试从端点取消部署策略之后，我注意到状态设置为“已取消部署，但存在失败”。

**解决方案：**

“已取消部署，但存在失败”状态表示无法在端点上执行使用取消部署脚本中的一个或多个规则取消部署策略的操作。无法在 CA Access Control 企业管理 中移除此策略状态。

要解决此问题，请手动删除策略版本的状态。

**更多信息：**

无法删除策略版本的状态 (p. 57)

# 无法删除策略版本的状态

**症状：**

某个策略版本在主机上无效，但我无法删除该策略版本的状态。这使我无法删除策略版本。

**解决方案：**

要解决此问题，必须手动删除策略状态。

要手动删除策略状态，请执行以下操作：

1. 删除端点上策略版本的状态。
   a. 在端点上执行以下 selang 命令：

      ```
      sr HNODE __local__
      ```

   b. 在输出的“策略状态”部分中找到策略名称，并记下策略的更新者。
   c. 在端点上执行以下 selang 命令：

      ```
      er HNODE __local__ policy(name(policyName#policyVersion)
      status(undeployed) updator(userName))
      ```

      ***policyName#policyVersion***

      定义要删除的策略版本的名称和版本号。

      ***userName***

      定义更新者的名称。

      端点上策略版本的状态将被删除。
2. 删除 DMS 上策略版本的状态。
   a. 在 DMS 上执行以下 selang 命令：

      ```
      sr HNODE hnodeName
      ```

      ***hnodeName***

      定义部署了策略版本的主机名称。

   b. 在输出的“策略状态”部分中找到策略名称，并记下策略的更新者。
   c. 在 DMS 上执行以下 selang 命令：

      ```
      er HNODE hnodeName policy(name(policyName#policyVersion)
      status(undeployed) updator(userName))
      ```

   DMS 上策略版本的状态将被删除。

### 示例：删除端点上策略版本的状态

以下示例将删除端点上名为 mypolicy、版本为 01 的策略的状态：

```
AC> sr HNODE __local__
(localhost)
HNODE '__local__' 数据
------------------------------------------------------------
被拒绝的访问权限     : R
审核模式          : 失败
所有者           : Domain\Administrator (USER)
创建时间          : 28-Feb-2010 12:34
更新时间          : 04-Mar-2010 05:10
更新者           : +policyfetcher (USER)
有效 UID         : superadmin
策略状态          :
    mypolicy#01   : 已部署              更新者: superadmin  更新时间: 04-Mar-2010
05:10
    偏差       : 未设置                 更新时间: N/A

AC> er HNODE __local__ policy(name(mypolicy#01) status(undeployed)
updator(superadmin))
(localhost)
成功更新 HNODE __local__
```

# 具有变量的规则无法部署在端点上

**症状：**

我创建了一个包含具有变量的规则的策略，并将该策略部署到了端点，但该规则未在端点上实施。

**解决方案：**

使用以下过程可排除策略部署问题：

1. 验证端点上 policyfetcher 部分中的 policyfetcher_enabled 配置设置的值是否为 1。

   如果此配置设置的值为 1，将运行 policyfetcher。如果 policyfetcher 未运行，则无法将策略发送到端点。

2. 检查 policyfetcher 日志中是否有错误。

   **注意：**policyfetcher 日志位于 *ACInstallDir*/Log 目录中，其中 *ACInstallDir* 是安装 CA Access Control 的目录。

3. 使用 CA Access Control 端点管理 验证是否在端点上定义了变量。

   **注意：**如果未在端点上定义该变量，则策略状态为“部署挂起”。

   如果未在端点上定义该变量，请创建一个包含 selang 规则（定义该变量）的新策略版本，并把该新策略版本部署到端点。

4. 验证是否满足以下条件：
   - 策略已分配给端点。

     如果策略未分配给端点，请使用 CA Access Control 企业管理 分配策略。
   - 策略的部署脚本不包含错误。

     如果策略的部署脚本包含错误，请创建一个修复错误的新策略版本，并将该新策略版本部署到端点。
   - 策略状态不是“不同步”。

     如果策略状态为“不同步”，表明变量值可能已在 CA Access Control 端点中发生更改。重新部署策略以清除“不同步”状态。
5. 审核部署信息以确定以下内容：
   - 端点已正确编译策略
   - 策略的 DEPLOYMENT 对象不包含任何部署错误

   如果策略未正确编译或 DEPLOYMENT 对象包含错误，请修复错误并重新部署策略。
6. 重新启动 CA Access Control。

# 内置变量未刷新

**症状：**

我在 CA Access Control 端点上更改了系统设置，但内置变量的值未更改为新系统设置的值。

**解决方案：**

使用以下过程可排除此问题：

1. 验证端点上 policyfetcher 部分中的 policyfetcher_enabled 配置设置的值是否为 1。

   如果此配置设置的值为 1，将运行 policyfetcher。如果 policyfetcher 未运行，则无法检查 CA Access Control 数据库中是否有更新的变量。

2. 如下所述验证 policyfetcher 在您更改系统设置之后是否发送了心跳：

   a. 在 CA Access Control 企业管理 中，单击“全局查看”，然后单击“全局查看”任务。

      将出现“搜索”屏幕。

   b. 如果需要，请定义用于查找特定数据子集的搜索条件，然后单击“执行”。

      与您定义的条件匹配的结果将按类别显示。

   c. 确定“上次状态”列中的更新时间晚于您更改系统设置的时间。

      如果端点的“上次状态”列中的更新时间早于您更改系统设置的时间，表明 policyfetcher 未发送心跳，且尚未检查变量值是否更新。

      **注意：**您可以通过更改 endpoint_heartbeat 配置设置来更改相同之间的时间间隔。

3. 重新启动 CA Access Control 并验证系统设置是否已更改。

# DNSDOMAINNAME 变量没有值

**症状：**

内置的 <!DNSDOMAINNAME> 变量没有值。

**解决方案：**

验证端点是否有 DNS 域。

要验证 Windows 端点是否有 DNS 域，请执行以下操作：

1. 打开命令提示窗口，然后运行以下命令：

   ```
   ipconfig/all
   ```

2. 验证主 DNS 后缀是否已设置为正确的值。

要验证 UNIX 端点是否有 DNS 域，请打开 /etc/resolv.conf 文件，并验证该域是否已设置为正确的值。

# DOMAINNAME 变量没有值

**症状：**

内置的 <!DOMAINNAME> 变量没有值。

**解决方案：**

验证端点是否已连接到域。

要验证 Windows 端点是否已连接到域，请执行以下操作：

1. 右键单击“我的电脑”，然后单击“属性”，单击“计算机名”选项卡，再单击“更改”。
2. 确定“隶属于域:”字段中有一个域。

要验证 UNIX 端点是否已连接到域，请执行以下操作：

1. 运行以下命令：

   ```
   ypcats hosts
   ```

2. 验证端点是否已连接到 NIC 域。

# HOSTNAME 变量名没有值

**症状：**

内置的 <!HOSTNAME> 变量没有值或者未完全限定。

**解决方案：**

验证端点是否有完全限定的主机名。

要验证 Windows 端点是否有完全限定的主机名，请执行以下操作：

1. 打开命令提示窗口，然后运行以下命令：

   ```
   ipconfig/all
   ```

2. 验证主 DNS 后缀是否已设置为正确的值。

要验证 UNIX 端点是否已连接到域，请在以下文件中检查是否已定义完全限定的主机名：

- /etc/hosts
- /etc/resolv.conf

# HOSTIP 变量没有值

**症状：**

内置的 <!HOSTIP> 变量没有值，或没有端点的所有 IP 地址。

**解决方案：**

验证 IP 地址是否存在于端点上。

要验证 IP 地址是否存在于 Windows 端点上，请执行以下操作：

1. 打开命令提示窗口，然后运行以下命令：

   ```
   ipconfig/all
   ```

2. 验证所有 IP 地址是否正确。

要验证 IP 地址是否存在于 UNIX 端点上，请执行以下操作：

1. 运行以下命令：

   ```
   ifconfig -a
   ```

2. 验证所有 IP 地址是否正确。

# 操作系统变量没有值

**症状：**

我已将某个 CA Access Control 操作系统变量定义为指向端点上的某个位置。当我在策略的规则中使用此变量时，CA Access Control 未实施该规则，因为该操作系统变量没有值。

**解决方案：**

验证该环境变量是否存在于端点上的操作系统中。

**验证该变量是否存在于操作系统中：**

1. 确定该 lt;eAC> 变量定义为操作系统变量（OSVAR 类型）。
2. 如下所述验证该操作系统变量是否存在于操作系统中：
   - (Windows) 打开命令提示符窗口，然后运行以下命令：

     set
   - (UNIX) 打开命令提示符窗口，然后运行以下命令：

     env

     **注意：**只有 root 用户才能运行此命令。

# 注册表变量没有值

**在 Windows 上有效**

**症状：**

我已将某个 CA Access Control 注册表变量定义为指向端点的某个位置。我尝试在策略的规则中使用此变量时，CA Access Control 未实施该规则，因为该注册表变量没有值。

**解决方案：**

注册表变量（REGVAL 类型的变量）必须指向 REG_SZ 或 REG_EXPAND_SZ 注册表类型。确定注册表变量中指定的注册表值是 REG_SZ 或 REG_EXPAND_SZ 类型。

# 第 8 章： 收集审核记录

此部分包含以下主题：



## 收集服务器未接收到某些审核日志消息

**在 UNIX 上有效**

**症状：**

我已将 CA Access Control 安装中的端点配置为将其本地审核日志路由到中央日志收集服务器，但服务器没有接收到所有审核日志。我已将 selogrd 配置为发送审核记录并将 selogrcd 配置为收集审核记录。

**解决方案：**

要排除 selorgd（CA Access Control 日志路由系统的发送器后台进程）故障，请执行以下操作：

- 查看 selogrd.cfg 文件。此文件用于配置 CA Access Control 将哪些审核消息路由到中央日志收集器。
- 查看每个端点的审核日志。如果审核日志中缺少某个审核事件，请查看 audit.cfg 文件。audit.cfg 文件用于配置 CA Access Control 将哪些审核事件写入审核日志。如果 audit.cfg 文件阻止 CA Access Control 将某个审核事件写入审核日志，则无法路由该审核事件。
- 将 selogrd（日志路由系统的发送器后台进程）配置为输出调试消息，然后再现问题。使用以下命令可将 selogrd 配置为输出调试消息：

  ```
  selogrd -d
  ```

# 收集服务器未接收到任何审核日志消息

**在 UNIX 上有效**

**症状：**

我已将 CA Access Control 安装中的端点配置为将其本地审核日志路由到中央日志收集服务器，但服务器没有接收到任何审核日志。我已将 selogrd 配置为发送审核记录并将 selogrcd 配置为收集审核记录。

**解决方案：**

验证 selogrcd 是否正在日志收集服务器上运行。

**注意：**如果 selogrcd 在很长一段时间内不运行，端点可能会放弃审核事件。

# SID 解析失败（事件查看器警告）

**在 Windows 上有效**

**症状：**

我查看 Windows 事件查看器的应用程序日志时，发现源自 CA Access Control 的警告事件说明将特定 SID 解析为帐户名称已经失败。

**解决方案：**

*安全标识符 (SID)* 是用于为操作系统标识用户或组的数字值。自主访问控制列表 (DACL) 中的每个条目都有一个 SID，用于标识访问权限被允许、拒绝或审核的用户或组。

在操作系统无法将 SID 转换为帐户名称时（例如：如果 SID 所指的用户或组不再存在），会出现此警告。请确定是否正确配置了有问题的系统和其相应的域控制器来进行 SID 解析。

# SID 解析超时（事件查看器警告）

**在 Windows 上有效**

**症状：**

我查看 Windows 事件查看器的应用程序日志时，发现源自 CA Access Control 的警告事件说明将特定 SID 解析为帐户名称已经超时。

**解决方案：**

*安全标识符 (SID)* 是用于为操作系统标识用户或组的数字值。自主访问控制列表 (DACL) 中的每个条目都有一个 SID，用于标识访问权限被允许、拒绝或审核的用户或组。

操作系统无法在指定的超时时间内将 SID 转换为帐户名称时警告才会出现。请确定：

- 是否正确配置了有问题的系统和其相应的域控制器来进行 SID 解析
- 是否正确配置了网络设置

您也可以通过更改以下注册表键中的 DefLookupTimeout 配置设置来延长超时时间：

```
HKEY_LOCAL_MACHINE\Software\ComputerAssociates\AccessControl\SeOSD
```

**注意：**增加 SID 解析超时可能会降低 CA Access Control 性能。

# 试图启动 selogrd 时收到错误代码 4631

**在 UNIX 上有效**

**症状：**

我试图启动 selogrd。selogrd 未启动，我收到以下错误消息：

```
错误 4631 (0x1217) 正在初始化 /opt/CA/AccessControl/bin/selogrd
```

**解决方案：**

在启动 selogrd 之前解析本地主机名。要解析主机名，请将主机名添加到操作系统 hosts 文件中，或者将主机名定义为 NIS 或 DNS。

# 审核日志记录在审核文件大小超过 2 GB 时停止

**症状：**

当审核文件大小超过 2 GB 时，CA Access Control 停止将审核记录写入审核文件。

**解决方案：**

当审核文件大小超过 2 GB 时，CA Access Control 无法将审核记录写入审核文件。可通过 logmgr 部分中的 audit_size 配置设置来指定 CA Access Control 审核文件的最大大小（KB）。

要将 seos.audit 文件的最大大小设置为 2 GB，请将 logmgr 部分中 audit_size 配置设置的值设置为 2097151。

# CA Access Control 写入审核日志时系统运行缓慢

**症状：**

在 CA Access Control 写入审核日志时，我的计算机运行缓慢。

**解决方案：**

当 CA Access Control 写入审核和跟踪数据时，可能会阻止系统中的大多数进程。要缩短 CA Access Control 写入审核数据和跟踪数据所需的时间，请执行以下操作：

- 仅对您需要的资源和访问设置审核模式。
- 仅在您需要时打开跟踪。
- 在速度最快的可用文件系统上存储审核文件、跟踪文件和 CA Access Control 数据库文件。

# 在主机分配有多个 IP 地址时不应用筛选

### 症状

我已将 audit.cfg 配置为使用主机名筛选分配有多个 IP 地址的主机上的 TCP 事件。应用筛选之后，我无法查看所有 IP 地址的 TCP 日志。

### 解决方案

在应用 audit.cfg 筛选后，审核系统会将主机名解析为主机 IP 地址，将主机 IP 地址解析为主机名。如果您为主机配置了多个 IP 地址，audit.cfg 只会筛选第一个 IP 地址。

要将 audit.cfg 筛选应用到所有 IP 地址，请仅在筛选中指定所有 IP 地址，而不指定主机名，例如：

```
TCP;*;192.168.30.138;*;R;P
TCP;*;192.168.30.139;*R;P
```

# 第 9 章： 调整性能

此部分包含以下主题：



## MALLOC_ARENA_MAX=1 未在 RedHat Linux 6.2 上工作

**在 RedHat Linux 6.2 上有效**

**症状：**

我注意到 UNAB uxauthd 代理过程超过允许的内存阈值且定期重新启动。

**解决方案：**

这种不稳定行为的原因与变量 MALOC_ARNEA_MAX 有关。要解决该问题，请执行以下步骤之一：

- 升级 glibc 库。
- 将内存阈值设置为最小 500MB：
  - 在 uxauth.ini 中修改 agent_vmemory_max 标记值
  - 如果 CA Access Control 已安装，在 seos.ini 中修改 ProcVSizeHigh 标记值
- 减少使用的线程数：
  - 将 uxauth.ini 文件中的 working_threads 标记值修改为 2

## CA Access Control 运行时性能下降

**症状：**

在 CA Access Control 运行时，我的计算机运行缓慢。停止 CA Access Control 后，我的计算机便可正常运行。

**解决方案：**

要诊断并改正性能问题，请排除性能问题 (p. 115)。

# CA Access Control 服务器上的系统负载过高

**症状：**

我需要减少 CA Access Control 服务器上的系统负载。

**解决方案：**

要减少系统负载，请执行以下操作：

- 避免在数据库中使用深层级结构。

  用户和资源的深层级结构要求系统负载获取并检查所有的依存关系。

- 避免对经常使用的目录使用常规规则。

  如果为经常使用的目录定义常规规则，CA Access Control 会检查许多系统操作。例如：如果您编写了用于保护 /usr/lib/* 的常规保护规则，CA Access Control 将检查系统中的每项操作。

- （仅限 Solaris）指定 CA Access Control 在文件属于进程文件系统 (/proc) 时跳过文件访问权限检查。

  要指定 CA Access Control 在文件属于进程文件系统时跳过文件访问权限检查，请确定 seos.ini 文件 [SEOS_syscall] 部分中的 proc_bypass 配置设置的值是 1。

  **注意：**有关 seos.ini 文件标记的详细信息，请参阅*《参考指南》*。

# 第 10 章： 排除 UNAB 问题

此部分包含以下主题：



## 无法安装 UNAB

**症状：**

我自定义了安装程序包，但当我试图在端点上安装 UNAB 时，安装失败。

**解决方案：**

使用以下过程可排除该问题。

1. 查看 UNAB 安装日志文件 uxauth_install.log 中是否包含错误。默认情况下，该文件位于以下目录中：

   ```
   /opt/CA/uxauth
   ```

2. 导出 UNAB 安装日志文件并将其发送到 CA 支持。
3. 以调试模式运行安装过程：
   - 对于本地程序包安装，请在 /tmp 目录中创建名为 seos_debug_on 的文件并为其指定调试级别（0-9 之间）。
4. 以调试模式运行本地程序包：
   - AIX－将 -e<*log_file_name*> 标志添加到 install 命令
   - HP-UX－查看 swinstall 为 swjob 生成的安装日志文件
   - Linux－将 -vv 标志添加到 install 命令
   - Solaris－将 -v 标志添加到 install 命令

# 排除 UNAB 注册故障

以下部分包含可用于排除在 Active Directory 的 UNAB 注册期间遇到的故障信息。

## 由于密码不正确，UNAB 注册失败

**症状：**

我尝试向 Active Directory 注册 UNAB 时，注册失败并显示以下错误消息：

获取初始凭据时预身份验证失败。使用 <Administrator> 的 Kerberos 预身份验证失败

**解决方案：**

由于管理员密码不正确，UNAB 注册失败。要排除此问题，请验证管理员密码并注册 UNAB。

## 由于时钟偏差不正确，UNAB 注册失败

**症状：**

我尝试向 Active Directory 注册 UNAB 时，收到以下错误消息：

获取初始凭据时时钟偏差过大。使用 <Administrator> 的 Kerberos 预身份验证失败

**解决方案：**

由于 Active Directory 和 UNAB 端点之间的时钟偏差大于配置值，UNAB 注册失败。

要解决此问题，请执行以下操作：

1. 手动将 UNAB 端点与 Active Directory 的时钟进行同步。
2. 将 uxauth.ini 中 [Agent] 部分下的 use_time_sync 标记值设置为 yes，以自动配置时间同步。

## 由于 NTP 服务器配置不正确，UNAB 注册失败

**症状：**

我尝试向 Active Directory 注册 UNAB 时，收到以下错误消息：

警告：未正确指定 NTP 服务位置

**解决方案：**

由于未正确配置网络时间协议 (NTP) 服务器，UNAB 注册失败。

要排除此问题，请将 uxauth.ini 中 [Agent] 部分下的 ntp_server 标记设置为指向 NTP 服务器。

## 由于配置无效，UNAB 注册失败

**症状：**

我尝试在 Active Directory 中注册 UNAB 时，收到以下错误消息：

初始化 Kerberos 5 库时出错。请检查 /opt/CA/uxauth/uxauth.ini。使用 <Administrator> 的 Kerberos 预身份验证失败

**症状：**

由于 uxauth.ini 文件中包含无效的 Kerberos 值，UNAB 注册失败。

要排除此问题，请运行 uxpreinstall 实用程序验证 Kerberos 配置。

## 由于缺少 DNS 设置，UNAB 注册失败

**症状：**

我尝试向 Active Directory 注册 UNAB 时，收到以下错误消息：

在 <domain_name> 域中找不到 LDAP 服务的 RR

**解决方案：**

由于未在 Active Directory 中配置 DNS 设置，UNAB 注册失败。

要排除此问题，请执行以下操作：

1. 运行 uxpreinstall 实用程序检查 DNS 设置。
2. 查看 uxpreinstall 实用程序的输出以确定 DNS 设置。
3. 如果不正确，请在以下文件中更新 DNS 设置：

   /etc/resolv.conf

## uxconsole -register 失败

**在 UNIX 上有效**

**症状：**

我运行 uxconsole -register 以注册 UNAB 端点时，出现以下错误消息：

```
没有服务器可用作与 Active Directory 通讯的 DC。
请检查 [ad] 部分中的 lookup_dc_list 和 ignore_dc_list 标记。
```

**解决方案：**

当 uxconsole 在 Active Directory 中注册 UNAB 端点时，将发现离端点物理位置最近的 Active Directory 站点。但是，uxauth.ini 文件 ad 部分中的 ignore_dc_list 配置设置会列出 UNAB 端点不与之通讯的域控制器。如果所发现 Active Directory 站点中的所有域控制器都列在 ignore_dc_list 配置设置中，注册将失败。

要解决此问题，请从 ignore_dc_list 配置设置中删除所发现 Active Directory 站点中所有域控制器的名称，并重新运行 uxconsole 实用程序。

**注意：**uxconsole 实用程序会将所发现 Active Directory 站点的名称写入 uxauth.ini 文件 ad 部分中的 ad_site 配置设置。有关 UNAB Active Directory 站点支持的详细信息，请参阅 *《实施指南》*。

# 未分发 UNAB 登录策略

**症状：**

我试图将 UNAB，登录策略部署到 UNAB 端点，但策略未分发。

**解决方案：**

要排除此问题，请执行以下操作：

1. 验证 UNAB 是否已在端点上启动：
   a. 在端点上打开命令提示符窗口。
   b. 运行以下命令：

      ```
      ./uxauthd.sh status
      ```

      将出现一条消息，通知您 UNAB 的当前状态。
2. 验证策略是否已下载到主机：
   a. 从端点上的命令提示符窗口中运行以下命令：

      ```
      ./uxconsole -status -detail
      ```

如果策略已部署到端点，输出的信息中将包括策略名称。

3. 查看企业管理服务器发送到 UNAB 端点的策略授权命令。
   - 从端点上的命令提示符窗口中运行以下命令：

     ```
     ./uxaudit -a
     18 Jan 2011 11:03:23 S UPDATE       TERMINAL   ac_entm_pers  338 10
     _default            acmanager.forwardinc.com auth terminal _default
     xuid(yaeyu01)access(read) (OS user)
     ```

   确定规则未被修改。
4. 搜索 syslog 文件中是否有消息队列通讯错误。
5. 确定用户帐户的登录权限和状态。
6. 在命令提示符窗口中运行以下命令：

   ```
   uxconsole -manage -show -user <AD_user_account>
   ```

# ReportAgent 无法将报告发送到企业管理服务器

**症状：**

我启动了 UNAB，并验证 ReportAgent 后台进程正在运行，但我无法在 CA Access Control 企业管理 中查看报告。

**解决方案：**

使用以下过程可排除此问题：

1. 检查“UNAB EP 与 ENTM 的通讯问题”部分中针对消息队列服务器通讯相关的错误消息的系统日志。
2. 如果要将报告数据发送到 CA Enterprise Log Manager，请验证是否将 accommon.ini 文件中 [ReportAgent] 部分下的 audit_enabled 标记设置为 1。
3. 启用 ReportAgent 调试。
4. 将 accommon.ini 文件中 [ReportAgent] 部分下的调试标记设置为 1
5. 查看 UNAB 报告调试文件 unab2xml.log。该文件位于以下目录：

   ```
   /opt/CA/AccessControlShared/log
   ```

6. 手动运行 ReportAgent 生成 UNAB 数据库快照：

   ```
   /opt/CA/AccessControlShared/bin/ReportAgent -debug 0 -task 2 –now
   ```

   **请注意下列事项：**

   - 在您手动运行 ReportAgent 之前，将路径“/opt/CA/AccessControlShared/lob”添加到 $LD_LIBRARY_PATH 中。
   - 在您手动运行 ReportAgent 之前，将 .dat 文件从 /opt/CA/AccessControlShared/data/audit2txt/ 目录中删除。
   - 有关 ReportAgent 实用程序调试模式的详细信息，请参阅《*参考指南*》。

# 注册 UNAB 主机时 Kerberos 预身份验证失败

**在 UNIX 上有效**

**症状：**

我使用 uxconsole -register 命令时，收到以下错误消息：

对 /opt/CA/uxauth/uxauth.ini 使用 krb5_set_config_files 失败：配置文件中缺少左大括号
使用 <Administrator> 的 Kerberos 预身份验证失败

**解决方案：**

uxauth.ini 文件中存在未设置的配置设置。要解决此问题，请确认 uxauth.ini 文件中的每个配置设置都具有值。

# 注册或启动 UNAB 时收到错误代码 2803

**在 UNIX 上有效**

**症状：**

我尝试在 Active Directory 中注册 UNAB 主机或启动 UNAB 时，收到以下错误消息：

无法打开 NSS 或创建 NSS 缓存。错误代码 2803。

**解决方案：**

/var 目录中的内存不足。要解决此问题，请确定 /var 中的内存使用率低于 95%，然后重试该命令。

# Active Directory 用户无法登录到 UNAB 端点

**在 UNIX 上有效**

**症状：**

具有 UNIX 属性的 Active Directory 用户无法登录到 UNAB 端点。

**解决方案：**

要解决该问题，请执行以下操作：

1. 确定用户的容器为以下容器之一：
   - user_container 配置设置中指定的容器。
   - user_container 配置设置中指定的容器下的子容器。

     **注意：**user_container 配置设置位于 uxauth.ini 文件的 AD 部分中。
2. 确定用户在 Active Directory 中具有 UID 和 GID。
3. 确定用户未被挂起。
4. 验证 UNAB 是否已在端点上启动：
   a. 在端点上打开命令提示符窗口。
   b. 运行以下命令：

      ```
      ./uxauthd.sh status
      ```

      将出现一条消息，通知您 UNAB 的当前状态。
5. 确定端点已在 Active Directory 中注册。

   **注意：**如果端点未在 Active Directory 中注册，请使用 uxconsole -register 实用程序注册该主机。
6. 如下所述在端点上停止您操作系统的名称或密码缓存后台进程：
   a. 停止 UNAB：

      ```
      ./uxauthd.sh stop
      ```
   b. 删除 NSS 缓存数据库：

      ```
      rm -rf /opt/CA/uxauth/etc/nss.db
      ```
   c. 检查您操作系统的名称或密码缓存后台进程是否正在端点上运行。

      例如：对于 Linux 或 Solaris 端点，检查 nscd 后台进程是否正在运行。对于 HP-UX 端点，检查 pwgrd 后台进程是否正在运行。
   d. 如果您操作系统的名称或密码缓存后台进程正在运行，请终止该进程。
   e. 启动 UNAB：

      ```
      ./uxauthd.sh start
      ```

7. 使用其他 Active Directory 用户帐户获取 Ticket Granting Ticket (TGT)。

   运行以下命令，以使用 Administrator 帐户连接到 Active Directory：

   ```
   ./uxconsole -krb -init Administrator
   ```

   **注意：**您可以使用代理 keytab 获取 TGT，例如：

   ```
   ./uxconsole -krb -init -k
   ```

8. 直接解析 Active Directory 用户帐户：

   - 运行以下搜索：

     ```
     ./uxconsole -ldap -search
     "(&(objectClass=user)(sAMAccountName=johndoe))"
     ```

     检查预期用户帐户名称与实际用户帐户名称之间的差异。

9. 在其他域中搜索用户帐户（如果适用）。

   - 运行以下命令：

     ```
     ./uxconsole -ldap -search -b DC=unabca,DC=test,DC=co,DC=il
     "(&(objectClass=user)(objectCategory=person))"
     ```

10. 验证 Active Directory 和 UNIX 上的用户帐户 UNIX 属性是否完全相同。

# 用户无法在 UNAB 端点上运行命令

**症状：**

我已成功登录到 UNAB 端点，且 UNAB 在与我的登录对应的 UNAB 审核文件 uxaudit 中创建了 P（已允许）记录。但是，我无法在端点上运行任何 UNIX 命令。

**解决方案：**

具有相同用户名但不同 UID 的用户已登录到同一端点，因此用户无法访问其 /home 目录。

要解决此问题，请执行以下操作：

1. 删除用户的 /home 目录。

   **注意：**/home 目录通常位于 /home/userName。

2. 要求用户登录到端点。

   现在为用户创建了一个新的 /home 目录。现在，用户可以在 UNAB 端点上执行 UNIX 命令。

# 无法在全局查看中查看 UNAB 端点

**在 UNIX 上有效**

**症状：**

我使用 CA Access Control 企业管理 来管理 UNAB 端点，但 UNAB 端点不显示在全局查看中。

**解决方案：**

验证 UNAB 端点是否可与分发服务器通讯。在 UNAB 端点上执行以下操作：

1. 验证 Distribution_Server 配置设置的值是否已设置为分发服务器计算机的名称。

   Distribution_Server 配置设置位于 accommon.ini 文件的 communication 部分中。

   **示例：** ssl://ds.comp.com:7243

   **注意：** 默认情况下，分发服务器位于企业管理服务器上。

2. 验证消息队列的密码是否正确。端点使用此密码与分发服务器进行通讯。请执行以下操作：

   a. 打开命令提示符窗口。

   b. 运行以下命令：

      ```
      acuxchkey -t pwd "password"
      ```

      ***password***

      定义消息队列密码。默认情况下，此密码是您在安装 CA Access Control 企业管理 时定义的通讯密码。

3. 重新启动 UNAB 代理，如下：

   a. 导航到 UNAB lbin 目录。

      默认情况下，此目录位于 /opt/CA/uxauth 下。

   b. 重新启动 UNAB 代理：

      ```
      ./uxauthd.sh restart
      ```

4. 验证消息队列服务器是否正在运行，如下：

   - Windows－验证 CA Access Control 消息队列服务是否正在运行。
   - UNIX－验证 tibemsd 进程是否正在运行

5. 检查 syslog 或事件查看器中是否有消息队列服务器通讯错误。

6. 设置消息队列服务器，以将与通讯相关的消息记录到日志文件中。请执行以下操作：
   - UNIX：
     a. 打开 pmd.ini
     b. 将 [endpoint_management] 部分中的 debug_mode 标记修改为 1
   - Windows：
   a. 导航到以下注册表键：

      HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Pmd\DMS_NAME\endpoint_management

   b. 将 debug_mode 标记的值修改为 1
7. 重新启动企业管理服务器以应用更改。查看 MS 目录中 endpoint_management.log 文件中的通讯消息。

   您已验证 UNAB 端点可与分发服务器进行通讯。

# 无法在 Linux s390 端点上启动后台进程

**在 Linux s390 和 Linux s390x 上有效**

**症状：**

我无法启动 uxauthd 或 ReportAgent 后台进程。

**解决方案：**

UNAB 在端点上找不到 Java 环境。要解决此问题，请执行以下操作：

1. 确定 accommon.ini 文件 global 部分中的 java_home 配置设置包含 Java 环境的路径。
2. 将 LD_LIBRARY_PATH 环境变量的值设置为 Java 环境的共享库的路径。

# 用户无法登录或更改密码

**在 UNIX 上有效**

**症状：**

我尝试在 UNAB 端点上登录或更改密码时，出现以下错误消息：

`passwd: 身份验证标记操作错误`

**解决方案：**

等待 uxauthd 响应密码更改请求时 PAM 模块超时。

要解决此问题，请执行以下操作：

1. 增加 uxauth.ini 文件 pam 部分中 pam_receive_timeout 配置设置的值。

   例如：pam_receive_timeout=100

2. 停止并重新启动 UNAB。

**注意：**有关 uxauth.ini 文件的详细信息，请参阅*《参考指南》*。

# 第 11 章： 排除 PUPM 故障

此部分包含以下主题：

# 紧急情况批准工作流

**症状：**

我想配置单步紧急情况工作流，以便验证请求适用的 PUPM 端点系统管理员得到通知，而不是用户经理。

**解决方案：**

您可以配置单步紧急情况工作流以指定紧急情况请求由系统管理员批准，而不是默认的批准人。

请按下列步骤操作：

1. 在 CA Access Control 企业管理 中，依次选择“用户和组”，“任务”，“修改管理任务”。

   将打开“修改管理任务: 选择任务搜索”窗口。

2. 从下拉选单选择“类别”并在文本框区域输入 *home*。单击“搜索”。

   CA Access Control 企业管理 显示与搜索条件相符的任务。

3. 选择“紧急情况 WF”任务，然后单击“选择”。

   “紧急情况 WF”属性窗口将打开。

4. 导航到“事件”选项卡，然后单击向右箭头。

   将打开“工作流映射”窗口。

5. 从工作流过程下拉选单中选择“SingleStepApproval”。

6. 在“主要批准人”部分中执行以下操作：

   a. 从“批准任务”下拉选单中选择“批准紧急情况特权帐户”。

   b. 从“参与人确定程序”下拉菜单中选择“自定义: PrivilegedAccountOwnerResolver”。

      将出现消息，通知您参与人确定程序配置参数未设置。

   c. 在“新参数名称”文本框中指定 SourceObject。

   d. 在“值”文本框中指定 TaskAdmin。

   e. 单击“添加参数”。

      CA Access Control 企业管理 添加批准人任务。

   f. 使用下列参数名和值，重复步骤 c 到 e：

      - SourceObjectAttribute—tblUser.manager
      - TargetType—USER

7. 单击“确定”。

您已配置单步紧急情况工作流，并将系统管理员定义为批准人。

# RunAs 密码使用方请求超时

**在 Windows 上有效**

**症状：**

我配置了一个 Windows RunAs 密码使用方，以便允许用户使用 RunAs 实用程序执行任务。在用户执行 RunAs 实用程序时，密码请求超时，用户无法执行该实用程序。

**解决方案：**

要解决此问题，请增加以下注册表项的值：

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Instrumentation\
Plugins\RunAsPlg\CommunicationWaitTimeout
```

该注册表项指定了密码使用方等待 PUPM 代理回复的时间（秒）。

## 示例：更改 CommunicationWaitTimeout 注册表项的值

以下示例将 CommunicationWaitTimeout 注册表项的值增加到 30：

```
AC> env config
AC(config)> editres CONFIG ACROOT section(Instrumentation\PlugIns\RunAsPlg)
token(CommunicationWaitTimeout) value(30)
(localhost)
成功设置标记。
```

# ODBC、OLEDB 或 OCI 数据库密码使用方请求超时

**在 Windows 上有效**

**症状：**

我在端点上配置了一个 ODBC、OLEDB 或 OCI 数据库密码使用方。当端点上的应用程序连接到数据库时，密码使用方会请求密码。但是，在应用程序尝试连接到数据库时，密码请求超时。

**解决方案：**

要解决此问题，请增加以下注册表项的值：

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Instrumentation\
Plugins\plugin\CommunicationWaitTimeout
```

***插件***

指定拦截连接尝试的插件的名称。

**值：**OCIPlg、ODBCPlg、OLEDBPlg

该注册表项指定了密码使用方等待 PUPM 代理回复的时间（秒）。

### 示例：更改 CommunicationWaitTimeout 注册表项的值

以下示例为 OCI 数据库密码使用方将 CommunicationWaitTimeout 注册表项的值增加到了 30：

```
AC> env config
AC(config)> editres CONFIG ACROOT section(Instrumentation\PlugIns\OCIPlg)
token(CommunicationWaitTimeout) value(30)
(localhost)
成功设置标记。
```

# PUPM SSH 设备超时

### 在 Red Hat 5 上有效

#### 症状

在我将日语版本的 Red Hat 5 配置为 PUPM SSH 设备端点并指定使用操作管理员用户登录名和操作管理员密码后，创建端点任务超时。

#### 解决方案

要解决该问题，请执行以下操作：

1. 导航到以下目录，其中 *ACServerInstallDir* 是您安装企业管理服务器的目录：

   *ACServerInstallDir*/Connector Server/conf/override/sshdyn

2. 打开 ssh_connector_conf.xml 文件进行编辑。
3. 在 <array name="oChangePassword"> 下添加以下项

```
<item>
    <param name="sCommand" value="set LANG=C" />
    <param name="iWait" value="500" />
    </item>
```

4. 保存并关闭文件。

# 请求的密码在未触发已批准工作流的情况下可用于签出

**适用于 SunOne**

**症状：**

在我输入对特权帐户密码的请求后，密码在事先没有得到我的管理员批准的情况下可用于签出。

**解决方案：**

默认情况下，当您将企业管理服务器安装在 SunOne 用户目录下时，会禁用工作流支持。您需要为用户启用工作流支持以提交特权帐户密码请求。

要对 SunOne 目录启用工作流支持，请执行以下操作：

1. 如果之前未执行此操作，请启用 Identity Manager 管理控制台。
2. 打开 Identity Manager 管理控制台。
3. 依次选择“环境”、“ac-env”、“高级设置”、“工作流”

   将打开“工作流属性”窗口。
4. 选择“启用”字段旁边的复选框。
5. 选择“保存”，然后选择“重新启动”以重新启动环境。

   现在您已对 SunOne 目录启用了工作流支持。

# 在创建 Windows Agentless 端点时收到“访问被拒绝”消息

**在 Windows 7 Enterprise 版上有效**

**症状：**

在我试图将 Windows 7 端点定义为 Windows Agentless 端点类型时，收到“访问被拒绝”消息且该过程失败。

**解决方案：**

端点创建过程失败，因为您指定的帐户不是 Administrator 帐户而是 Administrator 组的一个成员。

要解决此问题，请执行以下操作：

1. 登录到您想要以 Administrators 组成员身份进行管理的端点。
2. 依次选择“控制面板”、“用户帐户”、“更改用户帐户控制设置”。

   将打开“用户帐户控制设置”窗口。
3. 将通知级别设置为“默认”，然后单击“确定”。

   您可能需要重新启动计算机才能使更改生效。
4. 依次选择“管理工具”、“计算机管理”、“服务和应用程序”。
5. 右键单击“WMI 控件”，然后选择“属性”。

   将打开“WMI 控件属性”窗口。
6. 导航到“安全”选项卡。

   将打开命名空间导航窗口。
7. 选择“Root”，然后选择“安全”。

   此时将打开安全对话框。
8. 从“组或用户名称”部分中选择已通过身份验证的用户。
9. 从“允许”列中，清除“执行方法”复选框。
10. 单击“确定”以应用更改。

# 筛选 CA Access Control 端点（按属性）

**在 Windows 上有效**

**症状：**

我安装了几个分发服务器，以便使用 PUPM 端点分发通讯处理。我如何可以配置端点以与特定的分发服务器进行通讯？

**解决方案：**

通过使用端点详细信息选项，您可以配置每个端点以便与特定分发服务器进行通讯。

请执行以下操作：

1. 在 CA Access Control 企业管理 中，依次选择“特权帐户”、“端点”、“修改端点”。
2. 搜索要修改的端点并选择。

   此时打开“常规”选项卡。
3. 移到“信息”选项卡，并在“部门”字段中指定唯一名称。
4. 保存设置。
5. 在分发服务器上，停止所有 CA Access Control 服务。
6. 访问 Windows 注册表，并在以下路径中找到 ENDPOINT_DEPARTMENT 标记：

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl
   \Common\AgentManager\Plugins\AccountManager\QueryFilter
   ```
7. 将标记值设置为指定的部门名称。
8. 启动所有 CA Access Control 服务。

# 由于不正确参数，无法创建端点

**症状：**

在使用 PUPM 创建端点定义时，您可能收到表示“参数不正确”的错误。
错误：[常规] 端点无法在此端点类型中创建。
详细信息：端点*主机名*：参数不正确。

错误在 AgentManager.log 中记录，显示如下：

```
10/05/2013 12:37:54 acctmgr 2712> 使用 WMI ...
10/05/2013 12:37:54 acctmgr 2712> 使用帐户 CORP \UserName 连接到主机 <HOST> ...
10/05/2013 12:37:55 acctmgr 2712> IWbemLocator::ConnectServer 失败,
                                  错误 = 0x80070005（访问遭受拒绝。）
10/05/2013 12:37:55 acctmgr 2712> ValidateEndpointWMI 失败， 正在尝试
ValidateEndpointLDAP ...
10/05/2013 12:37:55 acctmgr 2712> 使用 LDAP ...
10/05/2013 12:37:55 acctmgr 2712> 使用帐户 CORP \UserName 连接到主机 <HOST> ...
10/05/2013 12:37:59 acctmgr 2712> IADsComputer::get_OperatingSystem 失败,
                                  错误 = 0x80070057（参数不正确。）
10/05/2013 12:37:59 acctmgr 2712> 无法验证端点 HOSTNAME -
                                  参数不正确。
10/05/2013 12:37:59 acctmgr 2712> 'validate ep' ret 失败
```

**解决方案：**

错误起因于错误的用户名。在以上错误日志中，在用户名“CORP \UserName”前的域名和斜杠之间出现错误的空格。

帐户名称的正确格式是“CORP\UserName”。确定从域名中删除结尾空格，并从用户名中删除前导空格。

# PUPM 导送程序轮询在负载平衡环境中不一致

**症状：**

我注意到在包含主服务器和负载平衡企业管理服务器的环境中工作时，[set the varname value at the book level] 导送程序轮询显示不一致的行为。

**解决方案：**

在包含负载平衡企业管理服务器的环境中工作时，您必须将导送程序轮询目录放置在网络的共享位置。您从两个企业管理服务器将完整路径名映射到共享目录。

**遵循这些步骤:**

1. 在 CA Access Control 企业管理 中，依次选择“用户和组”、“任务”、“修改管理任务”。
2. 搜索并选择“导入端点或帐户”任务。
3. 移动顶端的“选项卡”选项卡，并展开“导入端点或帐户”任务。
4. 在“轮询的文件夹(绝对路径)”字段中，指定 PUPM 导送程序轮询文件夹。例如：/Z:/Feeder。
5. 单击“确定”，然后单击“提交”。
6. 导航到以下路径，其中 *JBoss_HOME* 表示 JBoss 的安装目录：

   *JBoss_HOME*/server/default/deploy\/dentityMinder.ear/custom/ppm/default/feeder.propertie__
7. 指定完整路径名到共享文件夹，如下所示：
   FOLDER_FOR_POLLING=Z:/Feeder

   **重要说明！**对您的环境中每个企业管理服务器执行此程序。

# 第 12 章： 排除报告服务故障

此部分包含以下主题：



## 如何排除报告服务故障

通过 CA Access Control 报告服务，您可以在一个中央位置查看每个端点（用户、组和资源）的安全状态。在排除报告服务故障时，请依次检查每个组件。

以下过程可帮助您排除报告服务故障：

1. 根据端点上的操作系统，执行以下操作之一：
   - 在 UNIX 计算机上排除报告代理故障 (p. 95)
   - 在 Windows 计算机上排除报告代理故障 (p. 99)
2. 排除分发服务器故障 (p. 102)。
3. 排除 Boss 故障 (p. 103)。
4. 排除报告门户故障 (p. 104)。

### 在 UNIX 计算机上排除报告代理故障

**在 UNIX 上有效**

报告代理用于收集端点上本地 CA Access Control 数据库和任何策略模型数据库 (PMDB) 的排定快照，并以 XML 格式将快照发送到分发服务器上的报告队列。

**注意：**报告代理还执行其他任务。有关报告代理的详细信息，请参阅*《参考指南》*。

### 在 UNIX 计算机上排除报告代理故障

1. 验证库路径环境变量是否已正确设置。请执行以下操作：
   a. 使用 su 命令切换到 root 用户。
   b. 将库路径环境变量设置为 *ACSharedDir*/lib。默认情况下，*ACSharedDir* 是以下目录：

      ```
      /opt/CA/AccessControlShared
      ```

   c. 导出库路径环境变量。
2. 验证下列配置设置是否正确。这些配置设置位于 accommon.ini 文件的 [ReportAgent] 部分：

   **注意：**您可以使用 CA Access Control 端点管理 或 selang 命令验证配置设置的值。但是，在此过程中，建议您在配置环境中使用 selang 命令来更改配置设置的值。使用 selang 命令，您可以在此过程中更改配置设置，而无需停止并重新启动 CA Access Control。

   **reportagent_enabled**

   指定是否在本地计算机上启用报告 (1)。

   **默认值：**0

   **重要说明！**必须将此配置设置的值设置为 1，才能使报告代理自动运行。如果此配置设置的值为 0，报告代理不会将排定的数据库快照发送到分发服务器。但是，即使此配置设置的值为 0，您仍然可以在调试模式下运行报告代理。

   **schedule**

   定义生成报告并将报告发送到分发服务器的时间排定。

   您可以使用以下格式指定设置：time@day[,day2][...]

   **默认值：**00:00@Sun,Mon,Tue,Wed,Thu,Fri,Sat

   **示例：**“19:22@Sun,Mon”将在每个星期日和星期一晚上 7:22 生成报告。

   **send_queue**

   定义报告代理将本地数据库快照发送到的分发服务器上的消息队列名称。

   **默认值：**queue/snapshots

   **重要说明！**请勿更改此配置设置的默认值。

3. 验证下列配置设置是否正确。该配置设置位于 accommon.ini 文件的 [communication] 部分：

   **注意：**您可以使用 CA Access Control 端点管理 或 selang 命令验证配置设置的值。但是，在此过程中，建议您在配置环境中使用 selang 命令来更改配置设置的值。使用 selang 命令，您可以在此过程中更改配置设置，而无需停止并重新启动 CA Access Control。

   **Distribution_Server**

   定义分发服务器 URL。

   **注意：**TCP 通讯的默认端口为 7222，SSL 通讯的默认端口为 7243。您应当验证分发服务器 URL 是否为通讯类型指定了正确的端口号。

   **默认值：**无

   **示例：**ssl://172.24.176.145:7243。此 URL 将报告代理配置为使用 SSL 协议以 IP 地址 172.24.176.145 在端口 7243 上与分发服务器进行通讯。

4. 验证 seos.ini 文件的 [daemons] 部分中是否存在以下行：

   ```
   ReportAgent = yes, ACSharedDir/lbin/report_agent.sh start
   ```

   通过此行，可使报告代理后台进程在 CA Access Control 启动时自动执行。

   **注意：**默认情况下，*ACSharedDir* 目录位于 /opt/CA/AccessControlShared。

5. 停止 CA Access Control：

   ```
   secons -s
   ```

   CA Access Control 和报告代理将停止。

6. 浏览至以下目录：

   ```
   ACSharedDir/bin
   ```

7. 使用以下命令以调试模式运行报告代理：

   ```
   ./ReportAgent -debug 0 -task 0 -now
   ```

   **ReportAgent**

   运行报告代理。

   **-debug 0**

   指定以调试模式运行报告代理并在控制台上显示输出。

   **注意：**如果启用了报告代理后台进程，则不能以调试模式运行报告代理。

   **-task 0**

   指定报告代理收集有关 CA Access Control 数据库以及任何本地 PMDB 的信息并将这些信息发送到分发服务器。这些信息用于生成 CA Access Control 报告。

   **-now**

   指定立即运行报告代理。

8. 如下所述查看报告代理输出：
   - 查看输出中是否含有错误
   - 验证是否在“发送报告参数”部分中的“发送队列”和“报告文件”参数中指定了正确的名称。

9. 启动 CA Access Control：

   ```
   seload
   ```

   CA Access Control 和报告代理将启动。

### 示例：报告代理输出

以下报告代理输出显示的是“发送队列”和“报告文件”参数：

```
------------------------------------------------------------------------
发送报告参数:
------------------------------------------------------------------------
发送队列..................... queue/snapshots
报告文件.....................
/work/opt/CA/AccessControlShared/data/db2xml/ACDB.xml
------------------------------------------------------------------------
开始向队列“queue/snapshots”发送报告...
```

# 在 Windows 计算机上排除报告代理故障

### 在 Windows 上有效

报告代理用于收集端点上本地 CA Access Control 数据库和任何策略模型数据库 (PMDB) 的排定快照，并以 XML 格式将快照发送到分发服务器上的报告队列。

**注意：**报告代理还执行其他任务。有关报告代理的详细信息，请参阅*《参考指南》*。

### 在 Windows 计算机上排除报告代理故障

1. 验证下列配置设置是否正确。这些配置设置位于以下注册表键中：

   `HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\ReportAgent`

   **注意：**您可以使用 CA Access Control 端点管理 或 selang 命令验证配置设置的值。但是，在此过程中，建议您在配置环境中使用 selang 命令来更改配置设置的值。使用 selang 命令，您可以在此过程中更改配置设置，而无需停止并重新启动 CA Access Control。

   **reportagent_enabled**

   指定是否在本地计算机上启用报告 (1)。

   **默认值：**0

   **重要说明！**必须将此配置设置的值设置为 1，才能使报告代理自动运行。如果此配置设置的值为 0，报告代理不会将排定的数据库快照发送到分发服务器。但是，即使此配置设置的值为 0，您仍然可以在调试模式下运行报告代理。

   **schedule**

   定义生成报告并将报告发送到分发服务器的时间排定。

   您可以使用以下格式指定设置：time@day[,day2][...]

   **默认值：**00:00@Sun,Mon,Tue,Wed,Thu,Fri,Sat

   **示例：**“19:22@Sun,Mon”将在每个星期日和星期一晚上 7:22 生成报告。

   **send_queue**

   定义报告代理将本地数据库快照发送到的分发服务器上的消息队列名称。

   **默认值：**queue/snapshots

   **重要说明！**请勿更改此配置设置的默认值。

2. 验证下列配置设置是否正确。该配置设置位于以下注册表键中：

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Common\communication
   ```

   **Distribution_Server**

   定义分发服务器 URL。

   **注意：**TCP 通讯的默认端口为 7222，SSL 通讯的默认端口为 7243。您应当验证分发服务器 URL 是否为通讯类型指定了正确的端口号。

   **默认值：**无

   **示例：**ssl://172.24.176.145:7243。此 URL 将报告代理配置为使用 SSL 协议以 IP 地址 172.24.176.145 在端口 7243 上与分发服务器进行通讯。

3. 验证 CA Access Control 报告代理服务是否已启动。

   **注意：**您必须将 reportagent_enabled 配置设置设置为 1，才能将 CA Access Control，报告代理服务配置为自动启动。

4. 打开命令提示符窗口，然后停止 CA Access Control：

   ```
   secons -s
   ```

   CA Access Control 将停止，其中包括报告代理服务。

5. 使用以下命令以调试模式运行报告代理：

   ```
   reportagent -debug 0 -task 0 -now
   ```

   **reportagent**

   运行报告代理。

   **-debug 0**

   指定以调试模式运行报告代理并在控制台上显示输出。

   **注意：**如果启动了报告代理服务，则不能以调试模式运行报告代理。

   **-task 0**

   指定报告代理收集有关 CA Access Control 数据库以及任何本地 PMDB 的信息并将这些信息发送到分发服务器。这些信息用于生成 CA Access Control 报告。

   **-now**

   指定立即运行报告代理。

6. 如下所述查看报告代理输出：
   - 查看输出中是否含有错误
   - 验证是否在“发送报告参数”部分中的“发送队列”和“报告文件”参数中指定了正确的名称。
7. 启动 CA Access Control：

   ```
   seosd -start
   ```

   CA Access Control 和报告代理服务将启动。

### 示例：报告代理输出

以下报告代理输出显示的是“发送队列”和“报告文件”参数：

```
--------------------------------------------------------------------------
发送报告参数:
--------------------------------------------------------------------------
发送队列..................... queue/snapshots
报告文件..................... C:\Program
Files\CA\AccessControl\data\db2xml\ACDB.xml
--------------------------------------------------------------------------
开始向队列“queue/snapshots”发送报告...
```

## 库路径环境变量示例

以下示例是在 Linux 或 Solaris 计算机上设置和导出库路径环境变量：

```
LD_LIBRARY_PATH=${LD_LIBRARY_PATH}:/opt/CA/AccessControlShared/lib
export LD_LIBRARY_PATH
```

以下示例是在 AIX 计算机上设置和导出库路径环境变量：

```
export LIBPATH=$LIBPATH:/opt/CA/AccessControlShared/lib
```

以下示例是在 HP-UX 计算机上设置和导出库路径环境变量：

```
export SHLIB_LATH=$SHLIB_PATH:/opt/CA/AccessControlShared/lib
```

# 排除分发服务器故障

在分发服务器上，消息队列将接收报告代理从端点发送的信息。然后，消息驱动的 Java Bean (MDB) 将读取消息队列中的数据，并将其写入中央数据库。

### 排除分发服务器故障

1. (UNIX) 如下所述启动 Tibco EMS 管理工具：
   a. 浏览至以下目录：
      `/opt/CA/AccessControlServer/MessageQueue/tibco/ems/5.1/bin`
   b. 运行以下命令：
      ```
      ./tibemsadmin
      ```
2. (Windows) 如下所述启动 Tibco EMS 管理工具：
   a. 浏览至以下目录：
      `C:\Program Files\CA\AccessControlServer\MessageQueue\tibco\ems\5.1\bin`
   b. 运行以下命令：
      ```
      tibemsadmin.exe
      ```
3. 使用以下命令之一连接到当前环境：
   - 如果分发服务器在端口 7222（默认端口）上侦听报告代理，请使用以下命令：
     ```
     connect
     ```
   - 如果分发服务器在端口 7243 上侦听处于 SSL 模式的报告代理，请使用以下命令：
     ```
     connect SSL://7243
     ```
4. 输入用户名和密码。

   **注意：**默认用户名为 admin，默认情况下，密码是您在安装 CA Access Control 企业管理 或分发服务器时指定的通讯密码。

   此时将连接到分发服务器上的消息队列。
5. 输入下面的命令：
   ```
   show queues
   ```
   将显示分发服务器上的队列列表。
6. 在端点上打开命令提示符窗口。

7. (UNIX) 如下所述设置库路径环境变量：
   a. 使用 su 命令切换到 root 用户。
   b. 将库路径环境变量设置为 *ACSharedDir*/lib。默认情况下，*ACSharedDir* 为以下目录：

      ```
      /opt/CA/AccessControlShared
      ```

   c. 导出库路径环境变量。
8. (UNIX) 浏览至以下目录：

   *ACSharedDir*/bin
9. 在端点上运行报告代理。请执行下列操作之一：
   - (Windows) 运行以下命令：

     ```
     ReportAgent -report snapshot
     ```

   - (UNIX) 运行以下命令：

     ```
     ./ReportAgent -report snapshot
     ```

   报告代理将 CA Access Control 数据库和任何本地 PMDB 的快照发送到分发服务器上的报告队列。
10. 在报告代理运行时，可在 tibemsadmin 实用程序中观察到名为 queue/snapshots 的队列。

    如果该队列只增不减，说明 JBoss 可能未在运行。您必须排除 JBoss 故障。

## 排除 Boss 故障

JBoss Web 应用程序服务器环境包含消息驱动的 Java Bean (MDB)，这些 Java Bean 将从消息队列中读取数据，并将其写入中央数据库。中央数据库用于存储报告数据。

### 排除 JBoss 故障

1. 如下所述验证 JBoss 是否正确启动：
   - 如果您从命令提示符启动 JBoss，请在 JBoss 启动时查看初始输出。确定输出不包含任何错误。
   - 如果您将 JBoss 作为服务来启动，请在 JBoss 启动时使用日志文件或 tail 命令查看初始输出。确定输出不包含任何错误。
2. 打开以下文件并查看是否包含错误，其中 *JBossInstallDir* 是您安装 JBoss 的目录：

   *JBossInstallDir*/server/default/log/boot.log

   此文件列出了 JBoss 每次启动微内核时所执行的步骤。

3. 验证 JAVA_HOME 变量是否已设置到正确的位置。

   **注意：**如果 JAVA_HOME 变量已设置到正确的位置，但 JBoss 没有解析该变量，请将 JAVA_HOME 变量设置到更低的位置，例如：JDK 安装路径下的 bin 目录。

4. 打开以下文件并查看是否包含错误：

   *JBossInstallDir*/server/default/log/server.log

   此文件列出了 JBoss 在 JBoss Web 应用程序服务器环境中执行的操作。

   **注意：**每次启动 JBoss 时，它都会创建一个新的 server.log 文件。

5. 确定 JBoss 端口与其他服务上使用的端口不冲突。

6. （可选）如果 JNP 端口与其他服务相冲突，请如下所述将 JNP 端口 1099 更改为其他端口：

   a. 在文本编辑器中打开以下文件：

      *JBossInstallDir*/server/default/conf/jboss-service.xml

   b. 在以下部分中更改端口号：

      ```
      <!-- bootstrap JNP 服务的侦听端口。将此值设置为 -1 可在不使用 JNP 调用程序侦听端口的情况下运行 NamingService。->
      <attribute name="Port">1099</attribute>
      ```

   c. 保存并关闭文件。

7. （可选）如果 RMI 端口与其他服务相冲突，请如下所述将 RMI 端口 1098 更改为其他端口：

   a. 在文本编辑器中打开以下文件：

      *JBossInstallDir*/server/default/conf/jboss-service.xml

   b. 在以下部分中更改端口号：

      ```
      <!-- RMI 命名服务的端口，0 == 匿名 -->
      <!-- 属性名称="RmiPort">1098</attribute -->
      <attribute name="RmiPort">1098</attribute>
      ```

   c. 保存并关闭文件。

## 排除报告门户故障

通过报告门户，您可以访问分发服务器存储在中央数据库中的端点数据以生成内置报告，或查询数据并生成自定义报告。为执行此操作，它会使用 CA Business Intelligence。

### 排除报告门户故障

1. 确定您使用了正确的 URL 来访问报告界面 (BusinessObjects InfoView)。正确的 URL 为：

   http://*host*:*port*/businessobjects/enterprise115/desktoplaunch

2. (Windows) 确定您使用了正确的菜单选项来访问 InfoView。

   要访问 InfoView，请依次单击“开始”、“程序”、“Business Objects XI Release 2”、“BusinessObjects Enterprise”、“BusinessObjects Enterprise Java InfoView”。

3. 验证以下服务是否已启动：

   - Apache Tomcat
   - 中央管理服务器
   - 连接服务器
   - Crystal Reports 高速缓存服务器
   - Crystal Reports 作业服务器
   - Crystal Reports 页面服务器
   - Desktop Intelligence 高速缓存服务器
   - Desktop Intelligence 作业服务器
   - Desktop Intelligence 报告服务器
   - 目标作业服务器
   - 事件服务器
   - 输入文件存储库服务器
   - 值列表作业服务器
   - 输出文件存储库服务器
   - 程序作业服务器
   - 报告应用程序服务器
   - Web Intelligence 作业服务器
   - Web Intelligence 报告服务器

4. 测试 CA Access Control Universe 的连接。

   **注意：**如果 CA Access Control Universe 未显示在 BusinessObjects Designer 中，表明报告数据包可能未部署。有关如何部署报告数据包的详细信息，请参阅 *《实施指南》*。

## 测试 CA Access Control Universe 连接

CA Access Control Universe 是由 CA 提供的，用于简化从 CA Access Control 报告服务中央数据库的报告创建。

**注意：**有关 CA Access Control Universe 的详细信息，请参阅*《企业管理指南》*。

如果安装标准 CA Access Control 报告后出现有关报告服务连接的问题，应根据需要测试并修改连接。

**测试 CA Access Control Universe 连接**

1. 依次选择“开始”、“程序”、“Business Objects XI Release 2”、“BusinessObjects Enterprise”、“Designer”。

   将显示“用户身份验证”对话框，您可从中登录 BusinessObjects Designer。

2. 输入凭据，然后单击“确定”。

   将显示“快速设计”向导的欢迎屏幕。

3. 清除“启动时运行该向导”复选框，然后单击“取消”。

   将打开空的 Designer 会话。标题栏中将显示用户名和存储库名称。

4. 依次单击“文件”、“导入”，浏览至包含 CA Access Control Universe 的目录，选择“CA Access Control Universe”，然后单击“确定”。

   CA Access Control Universe 即成功导入，并在当前 Designer 窗口中打开。

   **注意：**CA Access Control Universe 存储在 CA Universe\CA Access Control 下指定为默认 Universe 文件存储的目录中。

5. 依次单击“工具”、“连接”

   将显示“向导连接”对话框。

6. 选择要测试的 Access_Control1 连接，然后单击“测试”。

   将显示一条消息，确认连接正在响应。如果连接未响应，您会收到一条错误消息。

7. 如果收到错误，请单击“编辑”修改以下连接设置：

   - 数据库中间件选择 - Oracle\Oracle 10\Oracle Client
   - 类型 - 受保护
   - 名称 - Access_Control1
   - 用户名 - *Oracle_adminUserName*

- 密码 - *Oracle_adminUserPass*
- 服务 - Oracle_TNS_Name

根据需要重复步骤 6 以测试连接。

# 报告服务器已关闭或不可访问

**症状：**

我尝试在 CA Business Intelligence 或 CA Access Control 企业管理 中查看报告时，收到以下错误消息：

报告服务器已关闭或不可访问。

**解决方案：**

要排除此问题，请执行以下操作：

1. 打开 JBoss 日志文件。JBoss 日志文件位于以下目录中，其中 *JBossInstallDir* 是您安装 JBoss 的目录：

   *JBossInstallDir*/server/default/log/server.log

   此文件列出了 JBoss 在 JBoss Web 应用程序服务器环境中执行的操作。

   **注意：**每次启动 JBoss 时，它都会创建一个新的 server.log 文件。
2. 在日志文件中找到错误原因。
3. 记下错误中出现的区分大小写的计算机名。

   您记录的名称必须与日志文件中的名称完全相符。
4. 打开 hosts 文件。默认情况下，hosts 文件位于以下目录中：
   - (UNIX) /etc/hosts
   - (Windows) C:\WINDOWS\system32\drivers\etc
5. 在该文件新的一行中，输入 IP 地址和区分大小写的计算机名，中间用空格分隔。

   计算机名是您在步骤 3 中所记录的计算机名。
6. 保存并关闭文件。

### 示例：hosts 文件

以下片段是 hosts 文件的示例：

```
127.0.0.1       localhost
```

# 使用 MS SQL 数据库时无法在 CA Business Intelligence 中查看报告

**症状：**

在我使用 MS SQL 数据库作为中央数据库时，无法在 CA Business Intelligence 中查看报告。我尝试查看报告时，收到以下错误消息：

连接失败

**解决方案：**

以下过程可帮助您排除 CA Business Intelligence 存在的问题：

1. 如下所述验证 BusinessObjects 的版本号：
   a. 打开以下 URL：

      `http://hostname:8080/businessobjects/enterprise115/adminlaunch/launchpad.html`

      ***hostname***

      定义报告门户主机的名称。

      将显示中央管理控制台登录页面。
   b. 输入用户名和密码，然后单击“登录”。

      将显示中央管理控制台。
   c. 依次单击“服务器”、“*hostname*”、“Web_IntelligenceReportServer”、“度量标准”。

      将显示 BusinessObjects 的版本号。
   d. 确定 BusinessObjects 的版本号为 11.5.8.1061 或更高版本，或者 11.5.10.1263 或更高版本。
2. 如下所述验证 CA Business Intelligence 的版本号：
   a. 在报告门户上打开以下文件：
      - (Windows) C:\Program Files\CA\SC\CommonReporting\version.txt
      - (UNIX) /opt/CA/SC/CommonReporting/version.txt
   b. 验证 CA Business Intelligence 版本是否为 2.1.13。

3. 如下所述验证数据库凭据是否正确：
   a. 依次单击“开始”、“程序”、“Microsoft SQL Server 2005”、“SQL Server Management Studio”。

      将显示 SQL Server 2005 登录页面。

   b. 键入您在为 CA Access Control 企业管理 准备数据库时所创建的 RDBMS 管理用户的用户名和密码。

   c. 单击“连接”。

      您将登录到 SQL Server Management Studio。如果您无法登录，则说明数据库凭据不正确。

4. 如下所述验证 *import_biar_config*.xml 文件是否具有正确的值：
   a. 打开您用于在报告门户上部署报告数据包的 *import_biar_config*.xml 文件。

   b. 验证下列属性的值是否与您在步骤 3 中指定的值相同：
      - <username> 与您输入的用户名相同。
      - <password> 与您输入的密码相同。
      - <datasource> 与您输入的数据库名称相同。
      - <server> 与报告服务器计算机的名称相同。

# 使用 Oracle 数据库时无法在 CA Business Intelligence 中查看报告

**症状：**

在我使用 Oracle 数据库作为中央数据库时，无法在 CA Business Intelligence 中查看报告。我尝试查看报告时，收到以下错误消息：

连接失败

**解决方案：**

以下过程可帮助您排除 CA Business Intelligence 存在的问题：

1. 如下所述验证 BusinessObjects 的版本号：
   a. 打开以下 URL：

      `http://hostname:8080/businessobjects/enterprise115/adminlaunch/launchpad.html`

      ***hostname***

      定义报告门户主机的名称。

      将显示中央管理控制台登录页面。

   b. 输入用户名和密码，然后单击“登录”。

      将显示中央管理控制台。

   c. 依次单击“服务器”、“*hostname*”、“Web_IntelligenceReportServer”、“度量标准”。

      将显示 BusinessObjects 的版本号。

   d. 确定 BusinessObjects 的版本号为 11.5.8.1061 或更高版本，或者 11.5.10.1263 或更高版本。
2. 如下所述验证 CA Business Intelligence 的版本号：
   a. 在报告门户上打开以下文件：
      - (Windows) C:\Program Files\CA\SC\CommonReporting\version.txt
      - (UNIX) /opt/CA/SC/CommonReporting/version.txt

   b. 验证 CA Business Intelligence 版本是否为 2.1.13。
3. 验证是否按照如下方式定义了 Oracle 系统环境变量，其中 *Oracle_home* 是您安装 Oracle 的目录：
   - ORACLE_HOME 指向 *Oracle_home* 目录
   - PATH 包含 *Oracle_home*/bin 目录
   - TNS_ADMIN 指向 *Oracle_home*/network/admin 目录
4. 如下所述验证是否正确定义了 TNS：
   a. 打开命令提示符窗口。

   b. 运行以下命令：

      `tnsping TNSname`

      ***TNSname***

      定义 TNS 的名称。

      如果您收到错误消息，表明未正确定义 TNS。

5. 如下所述验证您是否使用了正确的凭据访问数据库：
   a. 打开命令提示符窗口。
   b. 运行以下命令：

      sqlplus *user/password@TNSname*

      ***user***

      定义您在为 CA Access Control 企业管理 准备数据库时所创建的 RDBMS 管理用户的名称。

      ***密码***

      定义用户密码。

      如果您无法登录到 SQL 命令行，表明数据库凭据不正确。
6. 如下所述验证 *import_biar_config*.xml 文件是否具有正确的值：
   a. 打开您用于在报告门户上部署报告数据包的 *import_biar_config*.xml 文件。
   b. 验证下列属性的值是否与您在步骤 5 中指定的值相同：
      - <username> 与 *user* 相同
      - <password> 与 *password* 相同
      - <datasource> 与 *TNSname* 相同
7. (UNIX) 以您在安装 CA Business Intelligence 时指定的用户身份在步骤 4 和步骤 5 中运行命令。

   该用户是您在 CA Business Intelligence 安装向导的“CMS 数据库设置”页面中指定的。此步骤将验证用户是否对整个 *Oracle_home* 目录具有读取和执行访问权限。

# 无法在 CA Access Control 企业管理 中查看报告

**症状：**

我尝试在 CA Access Control 企业管理 中查看报告时，我的浏览器中出现 Business Objects 登录对话框和“隐私报告”图标。

**解决方案：**

您的浏览器正在阻止来自报告门户的 cookie。要解决此问题，请调整您浏览器中的 cookie 设置以允许来自报告门户的 cookie。

**注意：**隐私报告提供了有关浏览器阻止的 cookie 的详细信息。要显示隐私报告，请双击“隐私报告”图标。

# 附录 A： 故障排除和维护过程

此部分包含以下主题：



## 如何验证 CA Access Control 是否已正确安装

**在 Windows 上有效**

您应在安装 CA Access Control 后立即验证是否已正确安装。以下过程可帮助您验证 CA Access Control 是否已正确安装。

如果已成功安装 CA Access Control，则可以发现以下更改：

- 一个新项已添加至 Windows 注册表：

  `HKEY_LOCAL_MACHINE\Software\ComputerAssociates\AccessControl`

  当 CA Access Control 正在运行时，CA Access Control 密钥和子密钥受保护，您只能通过 CA Access Control 端点管理 或使用 selang 命令来修改这些密钥。但是，您不需要使用 CA Access Control 端点管理 或 selang 命令来读取这些密钥和值。

- 重新启动计算机时，将自动启动几项新的 CA Access Control 服务。这些服务包括始终安装好的 Watchdog、引擎和代理。根据您在安装过程中选择的选项，可能有其他服务（如任务指派）。所有 CA Access Control 服务的显示名称均以“CA Access Control”开头。您可以使用 Windows 服务管理器检查安装了哪些服务，并验证这些服务是否在运行。

# 如何排除资源访问问题

访问权限不正确是导致资源访问问题的最常见原因。资源访问问题的一个示例是，受保护资源的默认访问权限为 none，但 root 用户仍可访问受保护资源。以下过程可帮助您排除资源访问问题：

1. 将受保护资源的审核模式更改为全部审核：

   ```
   chres CLASS ResourceName audit(all)
   ```

   将审核模式更改为全部审核可使审核日志更易于读取。

2. 运行跟踪 (p. 116)并再现问题。
3. 查看跟踪文件和审核日志中是否出现了受保护资源。尝试通过文件中的信息来查明资源访问问题的原因。

   **注意：**SPECIALPGM 对象提供不受审核的跳过，但这些跳过会出现在跟踪文件中。

**注意：**要获得帮助，请通过 http://ca.com/worldwide 与技术支持联系。

# 如何排除连接问题

许多因素会影响 CA Access Control 计算机之间的连接。连接问题包括：无法连接到远程 CA Access Control 计算机，或者连接到远程计算机时超时。以下过程可帮助您识别连接问题的原因。

**注意：**要获得帮助，请通过 http://ca.com/worldwide 与技术支持联系。

1. 检查 CA Access Control 计算机中最近对以下内容的更改：
   - 加密密钥
   - 加密方法
   - TCP 和 UDP 端口
2. 查看 TCP、CONNECT、HOSTNET 或 HOST 类中新增或最近更改的规则。
3. 确定存在连接问题的端口。
4. 运行跟踪 (p. 116)并在跟踪文件中查看以下内容：
   - CA Access Control 因 TCP 规则或其他规则而阻止的连接
   - 存在连接问题的端口号旁边的代码，但 P（已允许）除外
5. 查看 CA Access Control 审核日志中是否有指向问题端口的 D（拒绝）记录。

6. 检查防火墙是否未阻止问题端口。
7. 查看您操作系统的日志文件中是否存在由于端口无法绑定而导致的错误消息。

**更多信息：**

更改 CA Access Control 代理通讯的端口号 (p. 120)

# 如何排除性能问题

以下过程可帮助您识别性能问题的原因。

**注意**：要获得帮助，请通过 http://ca.com/worldwide 与技术支持联系。

1. 确定性能问题的发生时间。性能下降是否发生在：
   - 操作系统启动时？
   - CA Access Control 启动时？
   - CA Access Control 运行一段时间后？
   - CA Access Control 或操作系统运行排定进程时？
   - (UNIX) 加载 CA Access Control 内核扩展时？
   - 加载 CA Access Control 后台进程或服务时？
2. 如果您确定 CA Access Control 导致了性能问题，请查明以下问题：
   - 性能下降时哪些进程使用的资源最多？
   - CA Access Control 进程是否在整个生命周期中都使用同一进程 ID？
   - 计算机上是否安装有任何第三方筛选驱动程序？
   - 计算机上是否安装有任何系统监视应用程序？
3. 检查 CA Access Control 数据库：
   a. 停止 CA Access Control。
   b. 检查数据库：

      ```
      dbmgr -util -all
      ```

   c. 重新编制数据库索引 (p. 118)。
   d. 重建数据库 (p. 119)。
   e. 重新启动 CA Access Control，并检查是否仍然存在该问题。

4. (Windows) 禁用驱动程序拦截：
   a. 停止 CA Access Control。
   b. 将 UseFsiDrv 注册表项的值更改为 0。UseFsiDrv 注册表项位于以下注册表键中：

      ```
      HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\AccessControl
      ```

   c. 重新启动 CA Access Control，并检查是否仍然存在该问题。
5. 运行跟踪 (p. 116)并再现问题。在跟踪文件中查看以下内容：
   - 短时间内的重复事件，例如：几秒内发生多次文件访问。
   - 已终止的进程。
   - 以下任一值：
     - ACEEH = -1
     - U = 负值

     这些值可能指定 CA Access Control 无法解析用户名或为资源分配值。

**注意：**有关改善 UNIX 计算机上 CA Access Control 性能的详细信息，请参阅 *《适用于 UNIX 的端点管理指南》*。

# 运行跟踪

运行跟踪可帮助您排除问题。CA Access Control 会将跟踪记录写入位于 *ACInstallDir*/log 目录中的 seos.trace 文件。

**运行跟踪**

1. 从跟踪文件中删除所有记录：

   ```
   secons -tc
   ```

2. 启动跟踪：

   ```
   secons -t+
   ```

3. 再现问题。
4. 停止跟踪：

   ```
   secons -t-
   ```

5. 查看跟踪文件。

**注意：**seosd 部分中的配置设置会配置跟踪文件。有关 seosd 部分的详细信息，请参阅 *《参考指南》*。

# 在 CA Access Control Web 服务组件上运行跟踪

**在 Windows 上有效**

在 CA Access Control Web 服务组件上运行跟踪可帮助您排除问题。例如：如果 CA Access Control 企业管理 无法连接到 DMS，您可以运行跟踪来查看这两个组件交换的消息。

CA Access Control 会将 Web 服务组件的跟踪记录写入在 WebService 部分的 logFileName 配置设置中定义的文件。此配置设置的默认值为 C:\Program Files\CA\AccessControlServer\WebService\log\WebService.log。

**在 CA Access Control Web 服务组件上运行跟踪**

1. 停止 CA Access Control 和 CA Access Control Web 服务。
2. 在以下位置创建一个注册表键：

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\WebService\TraceEnabled
   ```

3. 将该键的值设置为 1。
4. 启动 CA Access Control 和 CA Access Control Web 服务。

   跟踪将在 CA Access Control Web 服务组件上启动。
5. 再现问题。
6. 停止 CA Access Control 和 CA Access Control Web 服务。

   跟踪将在 CA Access Control Web 服务组件上停止。
7. 将该键的值设置为 0。
8. 查看跟踪文件。

# 重新编制 CA Access Control 数据库索引

因为对 CA Access Control 数据库进行了许多更新，所以数据库文件可能会碎片化。重新编制索引并重建数据库 (p. 119)有助于确保数据库在速度和可靠性方面的优化。请在每三到六个月执行一次的例行维护过程中以及遇到性能问题时重新编制数据库索引。

**注意：**在此过程中，CA Access Control 数据库会安装在默认位置 /opt/CA/AccessControl/seosdb (UNIX) 和 C:\Program Files\CA\AccessControl\Data\seosdb (Windows) 中。要执行此过程，您必须以 root 用户 (UNIX) 或管理员 (Windows) 身份登录。

**重新编制 CA Access Control 数据库索引**

1. 停止 CA Access Control。
2. 浏览至以下目录：
   - (UNIX) /opt/CA/AccessControl/seosdb
   - (Windows) C:\Program Files\CA\AccessControl\Data\seosdb
3. 备份数据库：

   ```
   dbmgr -backup backup_directory
   ```

4. 编制数据库索引：

   ```
   dbmgr -util -build seos_cdf.dat
   dbmgr -util -build seos_odf.dat
   dbmgr -util -build seos_pdf.dat
   dbmgr -util -build seos_pvf.dat
   ```

**注意：**要进一步减小 UNIX 计算机上数据库的大小，您可以使用 sepurgdb 实用程序从数据库中删除对未定义的记录的引用。有关 sepurgdb 实用程序的详细信息，请参阅*《参考指南》*。

# 重建 CA Access Control 数据库

因为对 CA Access Control 数据库进行了许多更新，所以数据库文件变得碎片化。重新编制索引 (p. 118)并重建数据库有助于确保数据库在速度和可靠性方面的优化。请在每三到六个月执行一次的例行维护过程中重建数据库。

**注意：**在此过程中，CA Access Control 数据库会安装在默认位置 /opt/CA/AccessControl/seosdb (UNIX) 和 C:\Program Files\CA\AccessControl\Data\seosdb (Windows) 中。要执行此过程，您必须以 root 用户 (UNIX) 或管理员 (Windows) 身份登录。

**重建 CA Access Control 数据库**

1. 停止 CA Access Control。
2. 浏览至以下目录：
   - (UNIX) /opt/CA/AccessControl/seosdb
   - (Windows) C:\Program Files\CA\AccessControl\Data\seosdb
3. 备份数据库：

   ```
   dbmgr -backup backup_directory
   ```
4. 从数据库中导出现有规则以及与用户相关的数据：

   ```
   dbmgr -export -l -f exported_filename
   dbmgr -migrate -r migrated_filename
   ```
5. 导航到以下目录并在其中创建名为 seosdb_new 的目录：
   - (UNIX) /opt/CA/AccessControl
   - (Windows) C:\Program Files\CA\AccessControl\Data
6. 在 seosdb_new 目录中创建数据库：

   ```
   dbmgr -create -cq
   ```
7. 将 *exported_filename* 和 *migrated_filename* 文件复制到 seosdb_new 目录。
8. 将从旧数据库中导出的现有规则以及与用户相关的数据导入新数据库：

   ```
   selang -l -f exported_filename
   dbmgr -migrate -w migrated_filename
   ```
9. 将 seosdb 目录重命名为 seosdb_old。
10. 将 seosdb_new 目录重命名为 seosdb。
11. 启动 CA Access Control。

# 更改 CA Access Control 代理通讯的端口号

CA Access Control 客户端应用程序（例如：selang、policydeploy 和 devcalc）与 CA Access Control 代理在端口 8891 上进行通讯。建议您不要更改此端口。如果确实需要更改此端口，请使用以下过程。

**更改 CA Access Control 代理通讯的端口号**

1. 在文本编辑器中打开以下文件：
   - (UNIX) /etc/services
   - (Windows) %SystemRoot%\drivers\etc\services
2. 将以下文件添加到该文件中：

   ```
   seoslang2 port-number/ tcp
   ```
3. 保存并关闭文件。
4. 重新启动 CA Access Control 后台进程或服务。

# 配置消息队列 TCP 端口

在安装 CA Access Control 企业管理 时，默认情况下将消息队列配置为使用 SSL 端口 (7243)。您可以更改此默认行为，并将消息队列配置为使用 TCP 端口 (7222)。

**连接到消息队列 TCP 端口**

1. 在企业管理服务器上，停止消息队列和 JBoss 服务器。
2. 打开文件 tibemsd.conf 进行编辑。此文件位于：

   ```
   C:\Program
   Files\CA\AccessControl\/MessageQueue/tibco/tibco/cfgmgmt/ems/data
   ```
3. 找到条目 listen=，删除其值，然后输入 tcp://7222。
4. 找到条目 authorization=，删除其值，然后输入 disabled。
5. 保存并关闭文件。
6. 打开文件 factories.conf 并找到标记 [SSLXAQueueConnectionFactory]。
7. 找到条目 url=，删除其值，然后输入 tcp://7222。
8. 保存并关闭文件。
9. 打开文件 tibco-jms-ds.xml 进行编辑。该文件位于：

   ```
   JBoss_HOME/server/default/deploy/jms
   ```
10. 搜索显示 SSL 端口号 (7243) 的所有值并将其替换为 TCP 端口号 7222。

11. 搜索显示值 SSLXA 的所有条目并将其替换为 XA。
12. 对以下两个条目添加注释 (<!--)：

```
com.tibco.tibjms.naming.security_protocol=ssl
com.tibco.tibjms.naming.ssl_enable_verify_host=false
```

13. 保存并关闭文件。
14. 启动消息队列和 JBoss 服务器。

# 提供给 CA 支持的信息

当您联系 CA 支持时，他们会要求您提供有关任何环境更改的信息以帮助其诊断问题原因。例如：主机和用户名更改以及操作系统的更改可能会影响 CA Access Control。CA 支持也可能要求您使用 CA Access Control 支持实用程序来提供其他诊断信息。

CA 支持会要求您提供以下信息：

- CA Access Control 版本
- 操作系统名称、版本、体系结构及更新级别
- 计算机上安装的任何 CA Access Control 修补程序的详细信息
- CPU 数量

**注意：**有关操作系统、版本、体系结构以及 CA Access Control 支持的更新级别的详细信息，请参阅《CA Access Control 兼容性列表》（可从 CA 支持上的 CA Access Control 产品页面获取）。

CA 支持可能会询问您以下问题：

- 该问题有什么影响？
- 第一次发生该问题是在什么时候？
- 该问题能否再现？
- 该问题发生之前，您是否在环境中添加、删除或更改了某些内容？
- 该问题发生之前，您是否重新启动了计算机？
- 该问题发生过多少次？
- 该问题发生时，系统上正在执行什么操作？例如：该问题是否是在您在执行某个特定进程或命令时发生？
- 该问题是持续发生，还是随机发生？
- 当您执行 CA Access Control 命令时是否会发生分段错误或访问冲突？

- 您认为 CA Access Control 引起该问题的原因是什么？
- 如果该问题是操作系统问题，您是否已将该问题报告给操作系统供应商？如果已经报告，您是否可以提供操作系统供应商的崩溃分析？

## 生成有关 Windows 端点的诊断信息

CA Access Control 支持实用程序会收集有关您的 CA Access Control 安装的信息，以便帮助 CA 支持诊断问题原因。请在“ACSupport”对话框中指定 CA Access Control 支持实用程序要收集的信息。

您可以收集以下系统信息：

- 系统信息报告
- 事件日志

您可以收集以下 CA Access Control 信息：

- 有关 CA Access Control 版本、主目录和 CA Access Control 服务状态的常见信息
- CA Access Control 注册表
- 用于审核、跟踪和共存实用程序的配置文件
- 审核和跟踪日志，包括本地 PMDB 或 DMS 的审核日志和检测跟踪
- 授权和缓存统计信息
- 计算机上安装的 CA Access Control 可执行文件和 DLL 的列表
- CA Access Control 数据库的快照，包括本地 PMDB 和 DMS

  **注意：**如果您收集 CA Access Control 数据库的副本，CA Access Control 支持实用程序会在创建数据库快照之前停止 CA Access Control，并在快照完成时重新启动 CA Access Control。

### 生成有关 Windows 端点的诊断信息

1. 导航到以下目录，其中 *ACInstallDir* 是您安装 CA Access Control 的目录：

   *ACInstallDir*\bin

2. 双击 ACSupport.exe。

   此时将打开“ACSupport”对话框。

3. 完成对话框，然后单击“继续”。

   CA Access Control 支持实用程序将创建安装快照，并将输出放置在 *ACInstallDir*\ACSupport 目录中。

# 生成有关 UNIX 端点的诊断信息

CA Access Control 支持实用程序会收集有关您的 CA Access Control 安装的信息，以便帮助 CA 支持诊断问题原因。如果您在快照中包括 CA Access Control 数据库，CA Access Control 支持实用程序会在创建数据库快照之前停止 CA Access Control，并在快照完成时重新启动 CA Access Control。

CA Access Control 支持实用程序始终收集有关 UNIX 端点的以下信息：

- seos.ini－CA Access Control 初始化文件
- tmpetc－CA Access Control /etc 目录中的文件，包括以下内容：
  - audit.cfg－审核筛选文件
  - auditroute.cfg－审核路由筛选文件
  - nfsdevs.init－包含每个操作系统的 NFS 主设备号默认值的文件
  - osver－操作系统版本
  - sereport.cfg－sereport 配置文件
  - serevu.cfg－serevu 配置文件
  - trcfilter.init－跟踪筛选文件
- versions.txt－包含关键 CA Access Control 二进制文件的版本的文件
- 一些操作系统文件，例如：某些变量文件

如果您指定 CA Access Control 支持实用程序收集有关 CA Access Control 数据库的信息，它将收集以下信息：

- seosdb－CA Access Control 数据库
- seosdb.tar－CA Access Control 数据库的压缩文件
- 组、主机、服务以及用户的后备数据库

如果您指定 CA Access Control 支持实用程序收集有关 CA Access Control 日志的信息，它将收集以下信息：

- tmplog－CA Access Control 日志文件
- log.tar－CA Access Control 日志目录的压缩文件

### 生成有关 UNIX 端点的诊断信息

1. 导航到以下目录，其中 *ACInstallDir* 是您安装 CA Access Control 的目录：

   *ACInstallDir*/lbin

2. 执行以下命令：

   ```
   ./support.sh [-db] [-log] [-all] [-none]
   ```

   **-db**

   收集有关 seosdb（CA Access Control 数据库）的信息，但不收集有关审核日志的信息。

   **-log**

   收集有关审核日志的信息，但不收集有关 seosdb 的信息。

   **-all**

   收集有关 seosdb 和审核日志的信息。

   **-none**

   不收集有关 seosdb 和审核日志的信息。

   **注意：**如果您不指定选项，CA Access Control 支持实用程序将以交互模式运行。

   CA Access Control 支持实用程序创建安装快照，并将输出放置在 *ACInstallDir* 目录中。