CA ControlMinder Premium Edition

版本说明

12.6.03

第三方通知

示例脚本和示例 SDK 代码

CA ControlMinder 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 ControlMinder Premium Edition
- CA ControlMinder
- 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 用户活动报告（以前是 CA Enterprise Log Manager）
- CA IdentityMinder

文档约定

CA ControlMinder 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）。 例如：下面的示例*既*可以表示用户名，*也*可以表示组名： `{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。 **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 ControlMinder 文档使用以下文件位置约定：

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

- *ACServerInstallDir*—默认 CA ControlMinder 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。

目录

第 1 章： 欢迎

欢迎使用 CA ControlMinder Premium Edition 12.6.03。本指南说明了新的增强、对现有功能所做的更改、支持的操作系统、系统要求、文档信息、安装和一般注意事项、公布的解决方案以及 CA ControlMinder Premium Edition 的已知问题。

此部分包含以下主题：

CA ControlMinder 安装介质

可从以下映像文件上获取 CA ControlMinder 组件。

以下映像文件包含端点组件：

- 适用于 Windows 的 CA ControlMinder 端点组件

  包含端点组件的 CA ControlMinder for Windows 安装文件。这些组件包括独立 Windows 计算机所需的核心 CA ControlMinder 功能、扩展核心功能（例如策略模型支持）所需的其他可执行文件和库、运行时 SDK 文件和库及 API 示例、大型机密码同步以及堆栈溢出保护 (STOP)。

- 适用于 UNIX 的 CA ControlMinder 端点组件

  包含端点组件的 CA ControlMinder for UNIX 安装文件。这些组件包括独立 UNIX 计算机所需的核心 CA ControlMinder 功能、扩展核心功能（例如策略模型支持）所需的其他二进制文件和脚本、API 库和示例、大型机密码同步以及堆栈溢出保护 (STOP)。

  此映像文件还包含用于 CA ControlMinder 企业管理 的 UNAB 安装文件。

所有版本的单个文档集

我们对两个版本提供同样的文档。因此，某些指南的某些部分仅适用于 CA ControlMinder Premium Edition。以下内容说明文档如何适用于 CA ControlMinder：

- 版本说明

  本指南中的一些信息仅适用于 CA ControlMinder Premium Edition 功能。

- 实施指南

  本指南中的一些信息仅适用于 CA ControlMinder Premium Edition 功能。

- 企业管理指南

  整个指南仅适用于 CA ControlMinder Premium Edition。

- Upgrade Guide（升级指南）

  本指南中的一些信息仅适用于 CA ControlMinder Premium Edition 功能。

- 实施指南

  整个指南适用于 CA ControlMinder Premium Edition。

- 端点管理指南：用于 Windows

  整个指南适用于 CA ControlMinder。

- 端点管理指南：用于 UNIX

  整个指南适用于 CA ControlMinder。

- 参考指南

  本指南中的一些信息仅适用于 CA ControlMinder Premium Edition 功能。

- selang 参考指南

  本指南中的一些信息仅适用于 CA ControlMinder Premium Edition 功能。

- 故障排除指南

  本指南中的一些信息仅适用于 CA ControlMinder Premium Edition 功能。

为了简化术语，在本文档中我们将此产品称为 CA ControlMinder。

第 2 章： 新增功能与经过更改的功能

此部分包含以下主题：

此版本中已解决的问题

此版本中包含的修复记录在版本修复列表中。您可以从 CA 支持上的 CA ControlMinder 最新维护版本页面中访问此修复列表。

第 3 章： 系统要求

此部分包含以下主题：

支持的操作系统

有关支持的操作系统的列表，请参阅“CA ControlMinder 兼容性列表”（可从 CA 支持的 CA ControlMinder 产品页上获取）。

CA ControlMinder 端点管理 要求

CA ControlMinder 端点管理 计算机的最低要求如下：

- **处理器** — (Windows) Pentium PC 2.66 GHz
- **内存**—2 GB RAM
- **可用磁盘空间**—安装目录中为 2 GB；%TEMP% (Windows) 或 /tmp (UNIX) 中为 3 GB

此外，还需要在 CA ControlMinder 端点管理 计算机中安装以下软件：

- **JDK**—Java 开发工具包 (JDK) 1.7 或更高版本
- **应用程序服务器**—JBoss Application Server 4.2.3.GA 版
- **CA ControlMinder**—最新版本的端点安装

在最终用户计算机上，您需要的最小屏幕分辨率为 1024 x 768，并需要以下浏览器作为 Web 浏览器：

- **Windows**—Microsoft Internet Explorer 6.x/7.x/8.x 或 Mozilla Firefox 2.x/3.0/3.5
- **Linux**—Mozilla Firefox 2.x/3.0/3.5

UNIX 端点要求

CA ControlMinder UNIX 端点的最低要求如下：

- **内存**－1 GB RAM（建议使用 2 GB）
- **可用磁盘空间**－250 MB（常规安装需 300 MB）

此外，CA ControlMinder 数据库也需要磁盘空间，该数据库是一个存储库，用于存储描述用户和用户组、受保护文件和其他资源的记录，以及允许对资源进行受控访问的授权。例如：一个可供一千名用户使用、包含一千个文件和五百条访问规则的数据库将占用大约 2 MB 的磁盘空间。

Windows 端点要求

CA ControlMinder Windows 端点的最低要求如下：

- **处理器**－基于 Intel 的 Pentium 4 PC，1.6 GHz
- **内存**－1-GB RAM
- **可用磁盘空间**－100 MB

此外，您也需要 CA ControlMinder 数据库的磁盘空间。例如：一个可供一千名用户使用、包含一千个文件和五百条访问规则的数据库将占用大约 2 MB 的磁盘空间。

策略模型数据库要求

除端点空间要求外，您还需要为计划在主机上创建的每个策略模型提供额外的磁盘空间。每个“策略模型”包含一个数据库，因此需要以 CA ControlMinder 数据库的相同操作方式来计算空间需求。

如果您要进行升级且所有策略模型数据库 (PMDB) 已准备就绪，请在升级前记录每个 PMDB 在 *ACInstallDir*/*policy_model_path*/pmdb_name 目录中使用的空间。使用以下计算方法估算出升级每个 PMDB 所需要的额外磁盘空间：

- *ACInstallDir*/policies/pmdb_name/subscribers.dat（大小）x 2
- *ACInstallDir*/policies/pmdb_name/updates.dat（大小）x 5 + 1000 KB

第 4 章： 文档

此部分包含以下主题：

指南

CA ControlMinder Premium Edition r12.6.01 的指南如下：

- 版本说明
- 实施指南
- 端点管理指南：用于 Windows
- 端点管理指南：用于 UNIX
- 企业管理指南
- 集成指南
- 升级指南
- 参考指南
- selang 参考指南
- 故障排除指南

注意：要查看 PDF 文件，您必须下载并安装可移植文档格式 (PDF) 阅读器。CA ControlMinder 文档需要 Adobe Reader 7.0.7 或更高版本。如果您的计算机中尚未安装 Adobe Reader，可从 Adobe 网站下载。

除 PDF 指南之外，还提供了 HTML 格式的 CA ControlMinder 指南，并且可从各种基于 Web 的界面访问联机帮助。

第 5 章： FIPS 遵从性

此部分包含以下主题：

FIPS 操作模式

CA ControlMinder 具有两种 FIPS 操作模式：仅 FIPS 模式和常规模式。在仅 FIPS 模式中，CA ControlMinder 仅使用那些遵从 FIPS 140-2 的加密功能。这意味着某些 CA ControlMinder 功能在仅 FIPS 模式中是禁用的。在常规模式中，CA ControlMinder 使用 FIPS 140-2 加密功能和非 FIPS 遵从功能。

注意：要在仅 FIPS 模式和常规模式之间切换，请使用加密区中的 *fips_only* 配置设置。

仅 FIPS 模式所不支持的操作系统

在 CA ControlMinder 支持的以下操作系统体系结构中不支持仅 FIPS 模式：

- Linux s390
- Linux Itanium (IA64)
- Solaris x64
- Windows Itanium (IA64)

FIPS 加密存储库

在仅 FIPS 模式中，CA ControlMinder 使用 CAPKI 加密库。在 UNIX 系统上，它使用操作系统加密库进行密码加密（“crypt”方式）。在常规模式中，除了非 FIPS 加密存储库外，CA ControlMinder 还使用 CAPKI 4.1.3 加密存储库。

使用的 FIPS 算法

CA ControlMinder 组件使用以下加密算法。不同的组件使用不同的算法。

- 在仅 FIPS 模式中：
  - SSL (TLS 1.0)—客户端/服务器通讯
  - CBC 模式中的 AES—PMD 更新文件 (Windows) 的加密 、双向密码历史记录 (Windows)
  - SHA-1—单向密码加密 (Windows)、受托程序、策略签名（高级策略管理）
- 在常规模式中：
  - CA ControlMinder r8 SP1 加密存储库（DES、Triple DES、AES、MD5 等）
  - SSL（SSL V2、SSL V3 和 TLS 1.0）—客户端/服务器通讯
  - SHA-1（通过 CAPKI）—用于受托程序的签名、策略的签名
  - AES（通过 CAPPKI）—用于在处理双向密码历史记录时进行密码验证

密钥和证书的存储

CA ControlMinder 按如下方式存储密钥和证书。

- 对称密钥按 eTrust Access Control r8 SP1 中的方式进行存储。
- 证书（主题证书、私钥和根证书）存储在文件系统中，由 CA ControlMinder 进行保护。

  注意：CA ControlMinder 通过使用 CA ControlMinder 对称密钥的 AES 对称加密（通过 CAPKI 存储库）来加密私钥。

受影响的功能 (UNIX)

FIPS 操作模式可能会影响以下 CA ControlMinder UNIX 功能：

功能	非 FIPS 模式	FIPS 模式
PMD 更新文件加密	默认对称密钥加密（双向）	已禁用
受托程序	CAPKI SHA-1 和 MD5	仅限 CAPKI SHA-1
双向密码加密	默认对称密钥加密	已禁用

功能	非 FIPS 模式	FIPS 模式
单向密码加密	操作系统的 crypt/bigcrypt 方法	操作系统的 crypt/bigcrypt 方法
PMD TNG 命令	默认对称密钥加密	已禁用
CA ControlMinder TNG 后台进程	默认对称密钥加密	已禁用
LDAP 密码加密使用（sebuildla -u -n）	默认对称密钥加密	已禁用
LDAP 密码加密生成 (seldapcred)	默认对称密钥加密	已禁用
TCP 通讯	默认的对称密钥加密（双向）或通过 SSL V2、SSL V3 或 TLS V1 的 CAPKI 套接字	通过 TLS V1 的 CAPKI 套接字
seversion 实用程序	CAPKI SHA-1	CAPKI SHA-1
受托程序（watchdog 和 seretrust）	CAPKI SHA-1	CAPKI SHA-1
高级策略管理策略分发	CAPKI SHA-1 签名、向后兼容、CA ControlMinder 内部 SHA-1 签名	仅限 CAPKI SHA-1 签名
selogrd 加密	默认的对称密钥加密和 MD5	已禁用
sechkey 密钥更改	默认对称密钥加密	已禁用
iRecorder 日志文件签名	MD5 加密	已禁用
报告代理	已启用	已禁用
SAM 代理	已启用	已禁用
DMS	已启用	UNAB 端点管理已禁用

注意：如果某个功能因 FIPS 操作模式而被禁用，则相关程序会输出错误消息并退出，或者在发生非交互式进程的情况下将错误消息写入系统日志。例如：报告代理或 SAM 代理。

受影响的功能 (Windows)

FIPS 操作模式可能对以下 CA ControlMinder Windows 功能产生影响：

功能	非 FIPS 模式	FIPS 模式
PMD 更新文件加密	默认对称密钥加密（双向）	CAPKI AES 对称密钥加密
密码历史记录（非双向）	另存为 CAPKI SHA-1。 通过 CAPKI SHA-1 进行密码验证而加密失败	另存为 CAPKI SHA-1。 仅通过 CAPKI SHA-1 进行密码验证
密码历史记录（双向）	默认对称密钥加密。 通过默认对称密钥加密进行密码验证	CAPKI AES 对称密钥加密。 仅通过 CAPKI AES 进行密码验证。
sechkey 密钥更改、密码历史记录	默认对称密钥加密对密码历史记录进行解密和加密	CAPKI AES 对称密钥加密对密码历史记录进行解密和加密
sechkey 密钥更改、策略模型	默认对称密钥加密对策略模型更新文件进行解密和加密	CAPKI AES 对称密钥加密对策略模型更新文件进行解密和加密
受托程序	CAPKI SHA-1 和 MD5	仅限 CAPKI SHA-1
大型机密码同步	已启用	已禁用
iRecorder	已启用	已禁用
TNG 集成	已启用	已禁用
高级策略管理策略分发	CAPKI SHA-1 签名、向后兼容、CA ControlMinder 内部 SHA-1 签名	仅限 CAPKI SHA-1 签名
报告代理	已启用	已禁用
SAM 代理	已启用	已禁用
DMS	已启用	UNAB 端点管理已禁用

注意：如果某个功能因 FIPS 操作模式而被禁用，则相关程序会输出错误消息并退出，或者在发生非交互式进程的情况下将错误消息写入系统日志。例如：报告代理或 SAM 代理。

您还应该考虑以下方面：

- 从非 FIPS 移至 FIPS 时，策略模型将*无法*读取旧命令。
- 从 FIPS 移至非 FIPS 时，策略模型将*可以*读取旧命令。
- 对于非双向密码历史记录，当不在 FIPS 模式中使用 crypt 时，则不会产生影响。crypt 仅适用于向后兼容。
- 对于双向密码历史，从非 FIPS 移动到 FIPS 时，CA ControlMinder 将无法解密旧密码。

第 6 章： 功能支持限制

此部分包含以下主题：

IPv6 支持

CA ControlMinder 可在单纯 IPv4 环境、单纯 IPv6 环境或 IPv4 和 IPv6 的混合环境中运行。

注意：(UNIX) selogrd 和 selogrcd 在仅 IPv6 环境中无法正常运行。

CA ControlMinder 当前不支持 IPv6 网络上的网络访问控制。这会对 HOST、CONNECT 和 TCP 类产生影响。

您可以将 IP 地址以 IPv6 格式指定给 CA ControlMinder，但 HOSTNET 类记录的掩码和匹配功能需要使用 IPv4 格式的地址。

产品重塑品牌限制

将以下产品组件重塑品牌为 CA ControlMinder：

- 安装消息
- 实用程序消息
- 用户界面页标题
- 显示名称
- 登录屏幕

未将以下产品组件重塑品牌，仍使用 CA Access Control：

- 产品路径名
- Selang 命令提示符
- 产品和程序文件名
- 注册表项
- 软件包名称

Windows 端点限制

本节介绍了 Windows 端点的功能支持限制。

x64 功能支持限制

以下是 Windows 2003 x64 上的已知限制：

- Unicenter TNG 迁移和集成
- 大型机密码同步
- 模拟截获（即类 SURROGATE 功能）（如果将 SurrogateInterceptionMode 设置为 1）

  重要说明！默认情况下，x64、IA64 和 x86 平台通过 RunAs 插件支持模拟截获（SurrogateInterceptionMode 设置为 0）。

  注意：有关 SurrogateInterceptionMode 注册表设置的详细信息，请参阅 *《参考指南》*。

IA64 功能支持限制

IA64 平台不支持以下功能：

- Unicenter TNG 迁移和集成
- 大型机密码同步
- STOP
- 报告代理
- SAM 代理
- SSL
- FIPS 140-2 遵从性

Windows Server 2008 功能支持限制

以下是 Windows Server 2008 上的已知限制：

- 模拟截获（即类 SURROGATE 功能）（如果将 SurrogateInterceptionMode 设置为 1）

  重要说明！默认情况下，x64、IA64 和 x86 平台通过 RunAs 插件支持模拟截获（SurrogateInterceptionMode 设置为 0）。

  注意：有关 SurrogateInterceptionMode 注册表设置的详细信息，请参阅 *《参考指南》*。

SAN 支持

当您将 CA ControlMinder 安装到以下系统时，CA ControlMinder 支持 SAN（存储区域网络）环境：

- 本地文件系统，当该 SAN 仅可从单个主机访问时用来保护 SAN 中的文件。

  注意：如果 SAN 可从多个主机访问，则将 CA ControlMinder 安装到可以访问该 SAN 的每个主机并使用每个安装来保护 SAN 中的文件。

- SAN 磁盘受以下限制：
  - CA ControlMinder 驱动程序必须安装到本地文件系统。
  - 每当启动或重新启动计算机时必须手工启动 SAN 磁盘中的 CA ControlMinder。当启动或重新启动计算机时不自动启动 CA ControlMinder。

    注意：在您将 CA ControlMinder 安装在 SAN 磁盘时先前的条件仅应用。如果您将 CA ControlMinder 安装在本地的文件系统并用其来保护 SAN 中的文件，那么在每次重新启动计算机时您 *不*需手工启动 CA ControlMinder。

如果 SAN 可从多个主机访问且 CA ControlMinder 安装在 SAN 中，而且想要将 CA ControlMinder 从其他主机安装到 SAN 的相同位置，请在开始之前考虑以下方面：

- CA ControlMinder 的新安装替代现有的 CA ControlMinder 安装并覆盖现有 CA ControlMinder 的配置文件和数据库。
- 必须在开始新安装之前停止现有 CA ControlMinder 的安装。

McAfee Entercept 缓冲区溢出

CA ControlMinder 的 STOP 功能与 McAfee Entercept 缓冲区溢出技术不兼容。

请关闭 CA ControlMinder STOP 功能或 McAfee Entercept 缓冲区溢出保护功能。

不支持短文件名规则（8.3 格式）

CA ControlMinder 不支持以短文件名（8.3 格式）创建的规则。定义以下任何类时，必须输入文件或目录的完整路径名：

FILE、PROGRAM、PROCESS、SECFILE、SPECIALPGM

以下是使用完整路径名的规则示例：

```
nr 文件 ("C:\program files\text.txt")
```

以下是*不*受支持的使用短路径名的规则示例：

```
nr 文件 ("C:\progra~1\test.txt")
```

UNIX 端点限制

本节介绍了 UNIX 端点的功能支持限制。

HP-UX 功能支持限制

以下是 HP-UX 操作系统上的已知 UNAB 和 CA ControlMinder 限制：

- seversion 实用程序不显示 SHA-1 签名。

HP-UX Itanium 和 RHEL Itanium 不支持 Unicenter 集成。

HP-UX Itanium (IA64) 和 Red Hat Linux Itanium IA64 不支持 Unicenter 集成。

Linux IA64 不支持 SAM 代理

Linux Itanium (IA64) 不支持 SAM 代理。无论在安装时如何选择，CA ControlMinder 都不会在这些操作系统上安装 SAM 代理。

注意：Linux IA64 也不支持 UNAB。

SAN 支持

将 CA ControlMinder 安装在本地文件系统上并用来保护 SAN（存储区域网络）上的文件时，如果该 SAN 可从安装有 CA ControlMinder 的单个主机进行访问，则 CA ControlMinder 支持 SAN 环境。

注意：如果 SAN 可从多个主机访问，则将 CA ControlMinder 安装到可以访问该 SAN 的每个主机并使用每个安装来保护 SAN 上的文件。

如果 SAN 可从多个主机访问且 CA ControlMinder 安装在 SAN 中，而且想要将 CA ControlMinder 从其他主机安装到 SAN 的相同位置，请在开始之前考虑以下方面：

- CA ControlMinder 的新安装替代现有的 CA ControlMinder 安装并覆盖现有 CA ControlMinder 的配置文件和数据库。
- 必须在开始新安装之前停止现有 CA ControlMinder 的安装。

注意：在 SAN 上安装 CA ControlMinder 时未指定其行为，它会从连接的多台主机执行。

UNAB 限制

本节介绍了 UNAB 端点的功能支持限制。

自定义脚本不支持多种选项更新

UNAB 自定义安装脚本不支持多种选项更新。您必须两次自定义安装脚本 -- 一旦接受许可，即可自定义安装选项。

在单向信任域环境中的帐户密码格式

在其他域而不是注册域使用 uxconsole 实用程序更改 Active Directory 帐户密码时，您必须使用以下命令格式：

```
uxconsole -krb -passwd user@DOMAIN
```

重要说明！域名必须以大写字母显示。

在 Linux IA64 上不支持 UNAB

目前，您无法在 Linux IA64 操作系统上安装 UNAB。

UNAB 不符合 FIPS140-2 和 IPV6 标准

目前，UNAB 不符合 FIPS140-2 和 IPV6 标准。

第 7 章： 安装注意事项

此部分包含以下主题：

支持的安装语言

您可以指定安装 CA ControlMinder 的语言。以下是您可以指定的受支持的语言 ID 及其代表的语言：

适用于 Windows 的 CA ControlMinder、适用于 UNIX 的 CA ControlMinder 和 UNAB 支持以下语言：

- 1033－英语
- 1041－日语
- 1042－韩语
- 2052－中文（简体）

仅端点组件版本

本版 CA ControlMinder 仅包含端点组件。以下端点组件包含在此版本中：

- 适用于 UNIX 的 CA ControlMinder 端点
- 适用于 Windows 的 CA ControlMinder 端点
- UNAB 端点

Windows 端点安装注意事项

本节介绍了在 Windows 端点上安装 CA ControlMinder 时应注意的事项。

在 Windows Server 2008 上安装、卸载或升级期间弹出重新启动消息

在 Windows Server 2008 上安装、卸载或升级 CA ControlMinder 时，可能会显示一个对话框，提示您完成此过程后需要重新启动。要想继续，请选择“确定”关闭对话框。

UNIX 端点安装注意事项

本节介绍了在 UNIX 端点上安装 CA ControlMinder 时应注意的事项。

Solaris 8 和 9 的 CA ControlMinder 安装注意事项

在 Solaris 8、Solais 9 上有效

要使用 Solaris 8 和 Solaris 9 操作系统上的本地程序包安装 CA ControlMinder，请在解压缩安装包之前完成以下步骤：

1. 将安装包复制到临时目录。
2. 执行以下命令：

   ```
   zcat _SOLARIS_126.tar.Z | tar xof -
   rm -f CAeAC/install/depend
   ```

3. 打开 /CAeAC/pkgmap 文件并找到以“1 i depend” 开头的行。
4. 删除行并保存文件。

   您现在可以自定义该程序包并安装 CA ControlMinder。

AIX 6.1 需要具有 TL3 或更高版本才能启动 CA ControlMinder

在 AIX 6.1 上有效

要在 AIX 6.1 上加载 CA ControlMinder，请验证是否已安装 TL3 或更高版本。

Linux390 的消息队列需要 J2SE 5.0 版

要在 Linux s390 和 s390x 端点上使用消息队列功能，请验证端点上是否安装了 J2SE 5.0 版或更高版本。通过消息队列功能，您可以将报告数据发送到报告门户，将审核数据发送到 CA Enterprise Log Manager。

注意：您可能需要在 accommon.ini 文件中配置 java_home 配置设置。有关详细信息，请参阅 *《实施指南》*。

x86_64bit Linux 上缺少兼容性库

默认情况下，x86_64 Linux 操作系统在安装时不应包括 32 位兼容性库。CA ControlMinder 端点要求库 libstdc++.so.6 存在于 rpm libstdc++ 的 usr/lib 目录中。

请在安装 CA ControlMinder 之前验证端点上是否存在此库。

CA ControlMinder 安装和卸载会重新启动 UNAB

在运行 UNAB 的端点上安装或卸载 CA ControlMinder 时，UNAB 代理 uxauthd 会停止并启动。

将 CA ControlMinder 和 UNAB 传播到新的 Solaris 区域

设置新的 Solaris 区域时，本地操作系统完全传播且运行程序包的后安装部分之前，您必须完成几个后安装步骤，您才可以将 CA ControlMinder 和 UNAB 传播到新区域。

注意：有关正确设置新区域的详细信息，请参阅 Oracle Documentation 网站上 Oracle 的《系统管理指南：Solaris Containers—资源管理和 Solaris Zones》。

在 Solaris 11 上安装 CA ControlMinder 的限制

由于 Solaris 11 的限制，在安装期间不会将 CA ControlMinder 包传播到非全局区域。我们建议您使用 Solaris 本地打包工具 (pkgadd) 分别在每个区域安装 CA ControlMinder。

UNAB 端点安装注意事项

本节介绍了安装 UNAB 端点时应注意的事项。

如果 CA_LIC 安装在非默认目录中，则会出现错误消息

在 Solaris 上有效

症状：

将 CA_LIC 安装到非默认目录之后，我试图安装 Solaris 主机上的 CA ControlMinder 和 UNAB。安装成功完成，但注册过程出现错误消息。

解决方案：

指定将 CA_LIC 组件安装到非默认目录时，错误消息出现，例如您指定 LIC_INSTALL_DIR 参数到 /work/CA 目录。要解决这个问题，请指定以下参数 CASHCOMP=/work/CA 并安装 UNAB。

在 Red Hat Enterprise Linux 5.8 上启用 UNAB SELinux 时，用户登录失败

在 Red Hat Enterprise Linux 5.8 上有效

如果启用 UNAB SELinux，Active Directory 用户无法登录到 Red Hat Enterprise Linux 5.8。

Solaris 8 和 9 的 UNAB 安装注意事项

在 Solaris 8、Solais 9 上有效

要在 Solaris 8 和 Solaris 9 操作系统上安装 UNAB，在解压缩安装包之前，必须完成以下步骤：

1. 将安装包复制到临时目录。
2. 执行以下命令：

   ```
   zcat _SOLARIS_Ux_PKG_126.tar.Z | tar xof -
   rm -f uxauth/install/depend
   ```

3. 打开 pkgmap 文件并找到以“1 i depend” 开头的行。
4. 删除行并保存文件。

   您现在可以自定义该程序包并安装 UNAB。

适用于 Linux 390 的 UNAB 需要安装 J2SE 5.0 版才能进行远程管理

要远程管理 Linux s390 和 s390x 端点，请验证端点上是否安装了 J2SE 5.0 版或更高版本。通过远程管理，您可以使用 CA ControlMinder 企业管理 管理 UNAB 端点。

注意：您可能需要在 accommon.ini 文件中配置 java_home 配置设置。有关详细信息，请参阅 *《实施指南》*。

第 8 章： 升级注意事项

此部分包含以下主题：

可以升级的版本

您可以将 CA ControlMinder 端点从以下版本升级到 12.6.03：

- 12.6.02
- 12.6.01
- 12.6
- 12.5.5

您无法将 CA ControlMinder 端点从以下版本升级到 12.6.03：

- 8.0 SP1 GA

  要升级 8.0 SP1 GA 端点，请在您升级到 12.6.03 之前，安装最新的 8.0 SP1 的 CR。

- 5.2 和 5.3

  要升级 5.2 或 5.3 端点，请在您升级到 12.6.03 之前安装最新的 8 SP1 的 CR。

Windows 端点升级注意事项

本节介绍了在 Windows 端点上升级 CA ControlMinder 时应注意的事项。

升级时可能需要重新启动

将端点从 r12.0 SP1 或更高版本升级到此版本时，不强制重新启动计算机。升级后，CA ControlMinder 会保留向后兼容性。但是，只有重新启动计算机后升级才算完成，所有新功能也只有在重新启动计算机后才能使用。

将端点从 r8.0 SP1 或 r12.0 升级到此版本时，必须重新启动计算机。

更改数据库的默认访问权限

现在 seosdb（CA ControlMinder 数据库）的默认访问权限为无。在 r12.5 SP2 和更低版本中，数据库的默认访问权限为读取。

注意：CA ControlMinder 内部进程对数据库具有完全访问权限，而 NT AUTHORITY\System 用户对数据库具有读取访问权限。

UNIX 端点升级注意事项

本节介绍了在 UNIX 端点上升级 CA ControlMinder 时应注意的事项。

默认安装位置

在 r12.0 中，默认安装位置有所更改，更改后的安装位置如下：

```
/opt/CA/AccessControl
```

FIPS 140-2 库升级

此 CA ControlMinder 版本使用 CAPKI 4.1.2，而非 ETPKI 3.2。升级将自动进行，如果有其他组件在使用 ETPKI 3.2 库，则升级时会保留计算机中的 ETPKI 3.2 库。为确定是否有其他组件在使用 ETPKI 3.2，CAPKI 将使用内部参考计数。如果此计数等于 0，ETPKI 3.2 会在升级时卸载。

UNIX 升级的系统范围审核模式

SEOS 类中的 SYSTEM_AAUDIT_MODE 属性为用户和企业用户指定了默认审核模式（系统范围的审核模式）。升级到 CA ControlMinder r12.5 SP1 或更高版本时，CA ControlMinder 将 SYSTEM_AAUDIT_MODE 属性的值设置为 DefaultAudit 配置设置（位于 lang.ini 文件的 [newusr] 部分中）的值。

注意：SYSTEM_AAUDIT_MODE 属性和 DefaultAudit 配置设置的默认值均为 Failure LoginSuccess LoginFailure。

授权识别资源组所有权

检查用户对资源的授权时，CA ControlMinder 会考虑资源组所有权。该操作在 12.0 中曾经介绍。在先前版本中，授权进程只考虑资源的所有者。

例如：对于一个默认访问权限为“无”，且所有者并非成员的 FILE 资源，您将其定义成已命名所有者的 GFILE 资源。在 CA ControlMinder r12.0 及更高版本中，命名的组所有者对该文件拥有完全访问权限。在较早版本中，没有用户可以访问该文件。

syslog 消息的优先级降低

以下 syslog 消息的优先级降到了信息级别（INFO，而非 ERROR）：

- CA ControlMinder 后台进程即将关闭。
- START-UP: CA ControlMinder PID=%d
- SEOS_load：use_streams=$use_streams unload_enable=$unload_enable
- 正在加载 CA ControlMinder 内核扩展。
- 已加载 $prodname 内核扩展。
- 启动 $SeosBinDir/seosd 后台进程。(CA ControlMinder)
- Watchdog 已启动。
- Watchdog 已初始化 Watchdog 扩展。

第 9 章： 一般注意事项

此部分包含以下主题：

Windows 端点注意事项

本节介绍了在 Windows 端点上使用 CA ControlMinder 时应注意的事项。

RunAs 管理员在 Windows Server 2008 上启动 CA ControlMinder

在 Windows Server 2008 上有效

要使用命令行选项 (seosd -start) 启动 CA ControlMinder，您需要具有管理员权限（如果启用了用户帐户控制 (UAC) 选项）。使用 RunAs 选项运行命令提示符，并指定具有管理权限的用户帐户。

卸载不删除 CA 许可文件

当您卸载 CA ControlMinder 时，不会删除 CA 许可文件。默认情况下，CA 许可文件位于 CA_license 目录（如 C:\Program Files\CA\SharedComponents\CA_LIC）。

UNAB 注意事项

本节介绍了使用 UNAB 时应注意的事项。

启用 SELinux 进行登录时未创建主目录

在 Linux 上有效

症状：

使用 SSH 客户端登录到 Linux 主机时，启用 SELinux 时，未创建我的帐户的主目录。

解决方案：

使用 SSH 客户端尝试登录时，未创建主目录。要解决此问题，请执行以下操作：

1. 打开 password-auth 文件。默认情况下，此文件位于以下目录中：

   `\etc\pam.d\`
2. 找到会话部分。
3. 在 pam_uxauth 部分之前添加下列行：

   会话需要 `pam_makehomedir.so`
4. 保存并关闭文件。

在 Red Hat Linux 上更改密码尝试失败

在 Red Hat Linux 上有效

症状：

在请求更改我的密码时，密码更改过程完成之后，我无法在主机上继续工作。使用 SSH 客户端或 Telnet 登录时，问题就会发生。

解决方案：

要解决该问题，请更改帐户密码，注销主机并使用新密码登录。

迁移后禁用本地用户帐户

将用户帐户完全迁移到 Active Directory 后，您可以通过在 etc/passwd 文件中帐户条目的开头添加星号 (*) 来禁用本地 UNIX 帐户。

不要将 unab_refresh_interval 标记值设置为短时间间隔

为避免 UNAB 性能问题，请不要将 unab_refresh_interval 标记值设置为短时间间隔。

不要将 Kerberos dns_lookup_realm 设置为 true

适用于 SSO 模式

建议除非有必要，否则不要将 Kerberos dns_lookup_realm 值设置为 true。如果设置为 true，Kerberos 会启动不必要的 DNS 搜索，这样会大幅减慢 UNAB 登录过程。

UNAB 用户无法根据指定的密码策略更改帐户密码

如果 UNAB 用户无法更改其帐户密码，请确定您使用的域控制器安全策略未禁止用户更改其帐户密码。

sepass 与 UNAB 端点集成

sepass 实用程序与 UNAB 集成在一起。通过此集成，用户可以在安装了 CA ControlMinder 和 UNAB 的端点上更改其 Active Directory 密码。

将 sepass 与 UNAB 集成：

- 确定您将 seos.ini 文件中的“change_pam”标志值设置为 **yes** 。配置此标志以指示 sepass 使用 PAM 界面更改密码。
- 确定您将 seos.ini 文件中的“auth_login”标志值设置为 **pam** 。配置此标志以指示 sepass 使用 PAM 界面验证现有密码。

注意：有关 seos.ini 初始化文件标志的详细信息，请参阅 *《参考指南》*。

使用 Active Directory 帐户登录到 UNAB

如果您要使用本地主机上之前不存在的 Active Directory 帐户登录到 UNAB，请执行以下步骤：

1. 使用以下命令向 Active Directory 注册 UNAB 主机：

   ```
   uxconsole -register
   ```

2. 使用以下命令激活 UNAB：

   ```
   uxconsole -activate
   ```

3. 创建 UNAB 登录授权（登录策略）或本地登录策略（users.allow、users.deny、groups.allow、groups.deny），以使 Active Directory 用户能够登录。

安装 UNAB 后，无法使用管理员帐户登录到 CA ControlMinder for UNIX

在端点上安装 UNAB 之后，无法使用 Active Directory 管理员用户帐户登录到适用于 UNIX 的 CA ControlMinder 端点。要解决此问题，您可以为此帐户创建 userPrincipleName。

第 10 章： 已知问题

此部分包含以下主题：

安装已知问题

本节介绍了 CA ControlMinder 组件的安装已知问题。

Windows 端点安装已知问题

本节介绍了 Windows 端点的安装已知问题。

从 MSI 文件进行安装时出现“找不到有效源”消息

升级 CA ControlMinder 时，可能会出现“找不到有效源”消息。如果当前使用的介质与最初用于安装 CA ControlMinder 的介质的 MSI 文件位于不同的路径中，将出现此消息。

要解决此问题，请添加名为“MediaPackage”的注册表字符串，并指定 CA ControlMinder msi 软件包的相对路径。在以下路径中添加注册表字符串：

```
HKLM\Software\Classes\Installer\Products\
CDAFB228040EC5F40AA08B5E852A6D61\SourceList\Media
```

例如：如果在 32 位 Windows 操作系统上安装 CA ControlMinder，则 msi 文件的完整路径为：E:\x86\，其中 E: 是可移动介质驱动器。在 MediaPackage 值中，指定值：\x86\

UNIX 端点安装已知问题

本节介绍了 UNIX 端点的安装已知问题。

当自定义几个区域设置的程序包时，非英语区域设置的本地程序包自定义失败

症状：

在非英语操作系统上自定义几个区域设置的 CA ControlMinder 或 UNAB 本地程序包时，自定义过程失败。

解决方案：

当前，您无法自定义支持几个非英语区域设置的 CA ControlMinder 和 UNAB 本地程序包。要解决此问题，请联系 CA 支持以获得在自定义程序包之前部署的修补程序。

RPM 软件包验证可能返回错误

验证 RPM 程序包安装时，可能会收到一些验证错误。

这些错误并不表明已安装的产品的功能存在问题，您可以放心地忽略它们。

客户端-服务器通讯模式不兼容

使用 non_ssl 或 all_modes 设置的客户端无法与使用 fips_only 通讯模式设置的服务器通讯。

Linux Z 系列的 API 库是 32 位

CA ControlMinder 为 Linux Z 系列 (s390x) 提供 32 位 API 库。

CA ControlMinder 不为 Linux Z 系列 (s390x) 提供 64 位库。

HP-UX 需要更新后的修补程序级别

在 HP-UX 上，CA ControlMinder 需要更新后的修补程序级别才能正确安装。建议使用以下操作系统修补程序：

- IA64 上的 11.23－日期为 2006 年 9 月或更晚的修补程序 PHSS_37492 或操作系统 QPK1123 包。
- PA-RISC 上的 11.11－支持“dld_getenv”的操作系统路径或日期为 2006 年 12 月或更晚的操作系统 QPR 包。
- PA-RISC 上的 11.23－日期为 2006 年 12 月或更晚的操作系统 QPK 包。

PAM 在具有较早版本 /lib64/libc.so.6 库的 Linux s390x 上无法正常工作

如果主机上的 /lib64/libc.so.6 库比编译 CA ControlMinder PAM 库所用版本更早，那么 Linux s390 和 s390x 中的 PAM 将不会工作。

该库的版本应为 2.3.2 或更高。

UNAB 端点安装已知问题

本节介绍了 CA ControlMinder 端点的安装已知问题。

当安装 CA ControlMinder 时，UNAB 重新启动两次

在 IBM AIX 上有效

在 IBM AIX 上安装 CA ControlMinder 时若 UNAB 已在运行，UNAB 会重新启动两次。这是因为 AIX 执行其他内核检查。

当本地安装自定义为在同一非默认位置安装 CA ControlMinder 和 UNAB 时，卸载失败

在 AIX 和 HP-UX 上有效

症状：

在我使用本地安装安装 CA ControlMinder 和 UNAB 并将安装目录自定义为非默认位置的同一路径之后，卸载 UNAB 失败。

解决方案：

卸载 CA ControlMinder 使 UNAB 安装损坏且失败。卸载失败，因为 CA ControlMinder 和 UNAB 被安装在同一目录中。将本地安装自定义到一个非默认目标文件夹时，建议您将产品名称（uxauth 或 UNAB）连接到目标路径。

UNAB 不支持 CA ControlMinder r8.0 SP1 和 r12.0 SP1

目前，您无法在 CA ControlMinder r8.0 SP1 和 r12.0 SP1 端点上安装 UNAB。此外，UNAB 和 CA ControlMinder 的版本或 Service Pack 必须完全相同。

已知升级问题

本节介绍了 CA ControlMinder 组件的升级已知问题。

Windows 端点升级已知问题

本节介绍了 Windows 端点的升级已知问题。

升级期间出现“没有足够的权限修改文件”消息

如果在升级 CA ControlMinder 端点时出现一则消息，通知您安装程序没有足够的权限修改文件，请确认该消息并继续升级。

UNIX 端点升级已知问题

本节介绍了 UNIX 端点的已知升级问题。

升级后 seaudit 和 sebuildla 出现权限被拒绝消息

在 AIX 上有效

在使用本地程序包升级之后，您可能会在使用 seaudit 和 sebuildla 实用程序时收到权限被拒绝的错误消息。

要解决此问题，请重新托管这些实用程序以完成升级。

r12.0 之前的版本必须使用最多 54 个字符作为加密密钥

如果您的环境包括早于 r12.0 版本的 CA ControlMinder，则必须使用最多 54 个字符作为加密密钥。

一般已知问题

本节介绍了 CA ControlMinder 组件的一般已知问题。

Windows 端点已知问题

本节介绍了适用于 Windows 的 CA ControlMinder 的已知问题。

卸载不会删除数据和日志目录

在 Windows 上有效

症状：

在我从系统中删除 CA ControlMinder 之后，我注意到卸载过程没有从以下路径中删除数据和日志目录：

```
\ProgramFiles\CA\AccessControl\
```

解决方案：

卸载过程不删除数据和日志目录。在过程完成之后，您可以手动删除他们。

Microsoft Internet Explorer 7.0 与 CA ControlMinder 的兼容性问题

由于 Microsoft Internet Explorer 7.0 与 CA ControlMinder 存在兼容性问题，浏览器可能会停止响应。要解决该问题，请安装 Microsoft Internet Explorer 8.0 或执行以下操作：

重要说明！请在开始此过程之前应用 Microsoft 软件修补程序 KB957388。您可以从 Microsoft 网站下载该软件修补程序。

1. 停止所有 CA ControlMinder 服务。
2. 打开命令行窗口，然后运行以下命令：

   ```
   net stop cainstrm
   ```
3. 从“运行”命令行窗口打开 regedit 实用程序。
4. 导航至以下路径：

   ```
   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSset\Services\cainstrm\parameters
   ```
5. 修改 ExcludeProcess 注册表项值以包括 iexplorer.exe 文件。
6. 从命令行窗口运行以下命令：

   ```
   net start cainstrm
   ```
7. 启动 CA ControlMinder 服务。

特权进程可以在未经授权的情况下保存和还原注册表树

在 Window Server 2003 及更高版本上，当进程获得特殊权限 SE_BACKUP_NAME 和 SE_RESTORE_NAME 时，它可以在未经 CA ControlMinder 授权的情况下保存和还原注册表树。

Windows x64 上的仅 FIPS 模式

现在，适用于 Windows 的 x64 CA ControlMinder 端点支持 CAPKI 4.1.2。但是，由于 RSA 的某个已知问题，在启用了 FIPS 的模式下运行 CAPKI 4.1.2 时，通讯会明显延迟。

selang 中的重命名 HOST 事件在 CA Enterprise Log Manager 报告中标记为未知事件

selang 中执行的重命名 HOST 事件在 CA Enterprise Log Manager 报告中显示为未知事件。

UNIX 端点已知问题

本节介绍了 CA ControlMinder for UNIX 的已知问题。

在 Solaris 8 上的 FTP 登录失败

症状：

我在 Solaris 8 计算机上，AD 用户的 FTP 登录失败。

```
530 登录不正确。
登录失败。
```

相同帐户凭据对于本机用户作用良好。

解决方案：

无。Solaris 8 的 ftpd 验证 /etc/shadow 和 NIS 中的帐户是否存在。较新 Solaris 版本的 FTP 实施没有此限制。

CAWIN 安装需要 Ncurses

在 Linux 64 位服务器上有效

在 Linux 64 位服务器上安装 CAWIN 之前，先安装 Ncurses 32 位。

在 serevu 后台进程运行时失败的登录事件不审核

在 VMware vCenter 4.0 u2 上有效

在 CA ControlMinder 安装在 VMware vCenter 版本 4.0 u2 上时，serevu 后台进程正在运行时，以下情况就会发生：

- 失败登录事件的登录记录不在审核文件中显示
- pam_seos_failed_login.log 文件大小是 0

要解决此问题，请执行以下操作：

1. 停止所有 CA ControlMinder 后台进程。
2. 浏览至以下目录：

   ```
   /etc/pam.d/
   ```

3. 编辑 system-auth 文件，删除所有到 pam_seos.so 的引用。例如：

   ```
   account required pam_per_user.so /etc/pam.d/login.map
   auth required pam_per_user.so /etc/pam.d/login.mapp
   password required pam_per_user.so /etc/pam.d/login.map
   session required pam_per_user.so /etc/pam.d/login.map
   ```

4. 编辑 system-auth-generic 文件，添加到 pam_seos.so 的引用。例如：

   ```
   password sufficient pam_seos.so
   auth       optional     pam_unix.so
   account   optional     pam_seos.so
   session   optional     pam_seos.so
   ```

5. 编辑 system-auth-local 文件，添加到 pam_seos.so 的引用。例如：

   ```
   password sufficient pam_seos.so
   auth       optional     pam_unix.so
   account   optional     pam_seos.so
   session   optional     pam_seos.so
   ```

6. 保存并关闭文件。
7. 启动 CA ControlMinder 后台进程。

SSH 登录不由 CA ControlMinder 或不由审核日志审核（启用 SElinux 时）

在 RedHat Linux Advanced Server 6 上有效

在 RedHat Linux Advanced Server 6 上，SSH 用户登录不由 CA ControlMinder 审核，因为 SElinux 默认策略不允许 SSHD 访问 /proc 文件系统。

要解决该问题，请运行 /opt/CA/AccessControl//lbin/sshd_policy.sh 脚本加载 SElinux 策略模块，以便允许访问 /proc。

无法在 Linux 上配置 JBoss JDBC 密码使用方

在 Linux 上有效

目前，您无法在 LInux 上配置 JBoss JDBC 密码使用方。

登录到 CA ControlMinder 需要启用 PAM_Login 标志

在 AIX 上有效

如果未启用 PAM_login 标志，CA ControlMinder 将无法正确检测到 Active Directory 用户帐户。

要解决此问题，请在设置的程序 (LOGINAPPL) 的日志中启用 PAM_login 标志。通过在 seos.ini 中的 [pam_seos] 部分下将 PamPassUserInfo 标记设置为 1，确定 seosd 后台进程接受来自 PAM 模块的登录请求。

您可以使用以下命令来设置登录标志：

```
er LOGINAPPL SSH loginflags(pamlogin)
```

如果在 /etc/shells 中没有定义默认 Shell，将不会记录用户会话

适用于键盘记录器

当用户使用 /etc/shells 中未定义的 shell 登录时，CA ControlMinder 不会记录用户会话。

在 PAM 处于活动状态时，不会为 FTP 和 SSH 宽限登录调用 segrace

激活 PAM 后，不会为 FTP 服务的宽限登录和 SSH 服务自动调用 segrace。

要为 FTP 解决此问题，请在 FTP 服务的 LOGINAPPL 记录中将 LOGINFLAGS 属性的值更改为 nograce。

要为 SSH 解决此问题，请不要从 PAM 调用 segrace， 而是从用户或操作系统启动脚本调用 segrace。

宽限期满后 CA ControlMinder 不会重置密码

在 HPUX 和 AIX 上有效

如果 CA ControlMinder 端点上安装了 UNAB，则 CA ControlMinder PAM 在用户密码宽限期满后不会调用 sepass 实用程序来重置帐户密码。

此问题会影响使用 loginflags(pamlogin) 的登录应用程序，例如：SSH 登录、rlogin、FTP 以及 Telnet。在 HPUX 和 AIX 上，CA ControlMinder 不会将 SSH 登录识别为登录操作。要解决此问题，请对 SSH 登录应用程序使用 loginflags(none)。

运行以下命令来设置标记：

```
er LOGINAPPL SSH loginflags(none)
```

Solaris 网络事件绕过不适用于某些进程

CA ControlMinder 在 Solaris 平台上不会为先于 CA ControlMinder 启动的进程绕过网络事件（绕过类型为 PBN 的 SPECIALPGM 记录）。

Stat 截获调用在 AIX 系统上不受支持

对于 STAT_intercept 标记设置为“1”的 stat 系统调用的文件访问检查在 AIX 系统上不受支持。

UNAB 已知问题

本节介绍了 UNAB 的已知问题。

UNAB 代理失去到信任域的连接

症状：

我在用户票单到期之前，配置了要到期的域安全策略 Kerberos 服务票单生命周期之后，UNAB 代理 (uxauthd) 失去到信任域的连接。

解决方案：

将 uxauth.ini 中的 tgt_renew_lifetime 标记值设置为小于 Kerberos 服务票单最大生命周期。

无法在首次登录时更改密码

在 Solaris 10 上有效

用户尝试使用 SSH 登录到 UNAB 主机时，试图在首次登录时更改帐户密码，密码更改操作则失败。

未记录到 AIX 的映射用户的失败登录尝试

在 AIX 上有效

症状：

在我作为映射的用户使用 SSH 尝试登录到 AIX UNIX 主机时，uxaudit 未记录失败的尝试。

解决方案：

如果用户输入不正确的密码，Seaudit 就不会记录映射用户的第一个失败登录尝试。uxaudit 记录随后的登录尝试。

下次登录时密码更改在 HP-UX 上失败

在 HP-UX 上有效

在 Active Directory 中，我选择了“用户必须在下次登录时更改密码”选项。在我使用 SSH 或 Telnet 登录时，用户无法登录或更改密码。

PAM 配置更改阻止用户登录

在 Red Hat Linux 5.0 及以上有效

症状：

我在 Red Hat Linux 上安装了 UNAB 和 CA ControlMinder，并配置了 PAM 配置文件，以便在控制字段中使用“value=action”语法。在我尝试登录到 Linux 主机时，登录操作被拒绝。

解决方案：

UNAB 不支持 PAM 配置文件中控制字段的“value=action”语法。

不正确的用户 ID 在单向信任域环境中取消注册 UNAB 之后显示

从单向信任域环境的 Active Directory 取消注册 UNAB 之后，会显示单向信任域的用户 ID 详细信息，即使他们不应出现。

在 AIX 上信任的用户 SSH 登录失败

症状：

我试图使用 SSH 登录到 AIX 5.3 端点，但登录尝试失败。

解决方案：

此错误是 AIX 和 SSH 版本若干组合的已知 IBM 问题。该问题已被 IBM 开发部门记录为 APAR（授权程序分析报告），编号：IV10231。

甚至将 watchdog_enabled 标记设置为 No 时，uxauthd 也启动

症状：

将标记 watchdog_enabled 设置为 no 且重新启动 UNAB 时，uxauthd 启动。

解决方案：

Watchdog 脚本忽略在第一次启动 uxauthd 之后对 watchdog_enabled 标记做出的更改。我们建议您在注册过程期间指定 *-n*，对标记做出更改，并分别启动 uxauthd.sh 脚本。

审核日志记录在尝试登录时使用本地帐户密码的登录

症状：

在我登录到 UNAB 且我的用户帐户存在于本地密码文件和 Active Directory 中时，审核日志显示以下记录：

```
<audit_record_date_and_time> A LOGIN map3
```

解决方案：

这是 UNAB 的已知问题。审核日志记录 A LOGIN，而不是 P LOGIN。

记录两次 Rlogin 条目

在 Linux 上有效

如果您登录到已使用 rlogin 安装了 UNAB 的主机，登录尝试将在审核中出现两次。

Microsoft Windows Server 2003 的热修复改进性能

在 Windows Server 2003 SP1、Windows Server 2003 64 位上有效

使用 LDAP_MATCHING_RULE_IN_CHAIN，LDAP 查询无法返回用于扩展搜索的 Active Directory 查询结果。

要解决该问题，为 MIcrosoft Windows 2003 Server 安装最新的 Service Pack，或通过将 wingrp_update_login 标记设置为 no 在登录期间禁用 UNAB 组更新。

注意：有关详细信息，请参阅 Microsoft 知识库文章 914828。

Uxpreinstall 实用程序无法验证主机名解析

在安装 UNAB 之后、注册 Active Directory 之前，uxpreinstall 实用程序无法验证主机名解析。

要解决此问题，请使用 -d 参数指定 Active Directory 域名。例如：

```
./uxpreinstall -d domain_name
```

审核记录中不显示 telnet 和 rlogin 程序

在 Linux、HP-UX 上有效

UNAB 审核记录不显示 telnet 和 rlogin 登录程序。在 Linux 中，UNAB 审核记录显示“remote”而不是 telnet 或 rlogin。在 HP-UX 上，UNAB 审核记录显示“login”而不是 telnet 或 rlogin。

uxconsole -register 和 -deregister 命令之间的间隔

如果要在 Active Directory 中注册 UNAB 主机之后又取消注册，建议您在取消注册主机之前等待域控制器复制所需的时间。

注意：如果取消注册 UNAB 主机，将删除未分发的策略。

新的域用户首次尝试登录时可能会失败

适用于 SSH

如果您在 Active Directory 中创建了一个用户后该新用户立即尝试登录到 UNAB 端点，则首次登录尝试将失败，但后续登录尝试会成功。首次登录尝试失败的原因是用户不为端点所知。但是，在失败的登录过程中，uxauthd 会将用户信息更新到本地 NSS 存储。后续登录尝试成功是因为现在端点已经知道该用户。

默认情况下，uxauthd 每小时更新一次 NSS 存储中的用户信息。如果新用户在 uxauthd 更新 NSS 存储之后再尝试登录到端点，登录将成功。

登录服务在 SSO 登录时跳过 PAM

多种登录服务在 SSO 登录时跳过 PAM。不会应用登录策略，也不会生成审核事件。

成功登录到主机后生成错误消息

适用于 Linux、AIX、HP-UX

UNIX PAM 流限制导致成功登录到 UNAB 主机的行为被记录为错误消息，在 syslog 文件中指出帐户身份验证失败。

使用 sepass 更改密码时出现密码不匹配消息

在 AIX 5.3 上有效

当映射用户尝试使用 sepass 更改帐户密码时，会出现密码不匹配错误消息。无论出现什么错误消息，都将在 Active Directory 上更改帐户密码。

Active Directory 用户无法在 Solaris 上更改密码

由于 Sun Solaris 密码限制，使用 Active Directory 帐户登录到 UNIX 主机的用户无法使用 Solaris passwd 工具更改其帐户密码。如果用户必须在首次登录时更改帐户密码，用户必须从 Solaris 之外的系统进行登录。

如果 UNAB 正在 UNIX 主机上运行，请使用以下命令来更改本地帐户密码：

```
passwd -r files username
```

如果 CA ControlMinder 正在 UNIX 主机上运行，请使用 sepass 实用程序来更改本地帐户密码。

模拟 Active Directory 用户不会创建审核记录

如果您使用 su 模拟 Active Directory 用户，则不会审核模拟尝试。

SFTP 会话的审核记录中显示 sshd 程序名称

使用 sftp 程序所做的登录会话审核记录可能会在程序字段中显示 sshd 后台进程而不显示 sftp 程序。

事件查看器中的 UNAB 条目包含空白字段

Windows 事件查看器中显示的 UNAB 事件具有空白字段。

不审核企业用户的 FTP SSO 登录

适用于 Solaris

Kerberized FTP 和 telnet 程序会跳过 PAM 堆栈，因此 UNAB 不会审核企业用户的 FTP 和 telnet SSO 登录。

取消注册启用了 SSO 的 UNAB 不会删除 keytab 文件中的记录

当您取消注册先前在启用了 SSO 的情况下注册的 UNAB 主机时，会从 Active Directory 中删除该计算机对象，但不会从 keytab 文件中删除相应的记录。如果您再次试图注册 UNAB 主机，将不会创建 Kerberos 票单。

要解决此问题，建议您不要取消注册 UNAB 主机，或者删除 keytab 文件（如果它仅由 UNAB 主机使用）。

HP-UX 不支持在密码中使用 @ 符号

在 HP-UX 上有效

由于 HP-UX 限制，请不要在 HP-UX 端点上的密码中使用 @ 符号。

HP-UX 不支持完全限定域名登录

在 HP-UX 上有效

您无法使用完全限定域名（例如：user@domain）登录到 HP-UX 主机。

文档已知问题

本节介绍了 CA ControlMinder 文档集的已知问题。

SDK 指南中的图形没有备用文本

SDK 指南中的图形没有备用文本。SDK 指南首次是随以前版本的 CA ControlMinder 一起发行的，并与 CA ControlMinder r12.5 文档一起提供。

PDF 文档需要 Adobe Reader 7.0.7

要以打印格式（PDF 文件）阅读 CA ControlMinder 文档，您必须安装 Adobe Reader 7.0.7 或更高版本。如果您的计算机中尚未安装 Adobe Reader，可从 Adobe 网站下载。

注意：Adobe Reader 在 HP-UX Itanium (IA64) 和 Red Hat Linux Itanium IA64 上不可用。