CA Performance Center

Single Sign-On 用户指南

2.4

ca technologies

本文档包括内嵌帮助系统和以电子形式分发的材料（以下简称“文档”），其仅供参考，CA 随时可对其进行更改或撤销。

未经 CA 事先书面同意，不得擅自复制、转让、翻印、透露、修改或转录本文档的全部或部分内容。本文档属于 CA 的机密和专有信息，不得擅自透露，或除以下协议中所允许的用途，不得用于其他任何用途：(i) 您与 CA 之间关于使用与本文档相关的 CA 软件的单独协议；或者 (ii) 您与 CA 之间单独的保密协议。

尽管有上述规定，但如果您为本文档中所指的软件产品的授权用户，则您可打印或提供合理数量的本文档副本，供您及您的雇员内部用于与该软件相关的用途，前提是所有 CA 版权声明和标识必须附在每一份副本上。

打印或提供本文档副本的权利仅限于此类软件所适用的许可协议的有效期内。如果该许可因任何原因而终止，您应负责向 CA 书面证明已将本文档的所有副本和部分副本已退还给 CA 或被销毁。

在所适用的法律允许的范围内，CA 按照“现状”提供本文档，不附带任何保证，包括但不限于商品适销性、适用于特定目的或不侵权的默示保证。CA 在任何情况下对您或其他第三方由于使用本文档所造成的直接或间接的损失或损害都不负任何责任，包括但不限于利润损失、投资受损、业务中断、信誉损失或数据丢失，即使 CA 已经被提前明确告知这种损失或损害的可能性。

本文档中涉及的任何软件产品的使用均应遵照有关许可协议的规定且根据本声明中的条款不得以任何方式修改此许可协议。

本文档由 CA 制作。

仅提供“有限权利”。美国政府使用、复制或透露本系统受 FAR Sections 12.212、52.227-14 和 52.227-19(c)(1) - (2) 以及 DFARS Section 252.227-7014(b)(3) 的相关条款或其后续条款的限制。

版权所有 © 2014 CA。保留所有权利。此处涉及的所有商标、商品名称、服务标识和徽标均归其各自公司所有。

CA Technologies 产品引用

本文档引用以下 CA Technologies 产品：

- CA Performance Center
- CA Infrastructure Management Data Aggregator
- CA Network Flow Analysis
- CA Application Delivery Analysis
- CA Unified Communications Monitor

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： 在 CA Performance Center 中自定义身份验证

此部分包含以下主题：

CA Single Sign-On

*单点登录*是用于 CA Performance Center 和所有受支持数据源的身份验证方案。在用户经身份验证有权访问 CA Performance Center 之后，他们无需再次登录即可在控制台和注册的数据源中导航。

通过在各个产品界面之间实现导航，对于正在分析性能和状态数据的操作员来说，单点登录能够确保实现无缝的深入查看体验。例如，如果用户登录到 CA Performance Center，然后沿着深入查看路径访问数据源界面，该用户无需再次登录。

CA Performance Center 使用一种分布式体系结构。在已安装支持的数据源或 CA Performance Center 的每个服务器上，会自动安装一个单点登录 Web 站点实例。使用分布式体系结构，用户可以通过登录到运行各个 CA 数据源产品的服务器来登录这些产品。

CA Performance Center 身份验证和安全

单点登录向 CA Performance Center 和支持的数据源提供身份验证服务。它还支持外部身份验证方案，如 LDAP 和 SAML 2.0。通过这种支持，可以在企业范围内将 CA Performance Center 和其他 CA 数据源产品集成到相同的身份验证方案中。

单点登录安全审核功能可记录有关登录用户和登录时间的信息。在 Linux 服务器上，日志保存于以下位置：
`[安装目录]/PerformanceCenter/sso/logs`

在安装数据源的 Windows 服务器上，日志保存于以下目录中：
`[安装目录]\Portal\SSO\logs`

身份验证方法

单点登录组件提供了登录页，该登录页在 CA Performance Center 和数据源产品中支持用户身份验证。单点登录支持以下身份验证方法：

- 产品身份验证，该身份验证基于用户帐户
- LDAP
- 安全声明标记语言 (SAML) 2.0

CA Performance Center 管理员可以修改单点登录单个实例的设置。例如，可以在单点登录中设置 LDAP 身份验证。也可以使用安全套接字层 (SSL) 配置可选加密，或更改默认虚拟目录。

注意：由于使用分布式体系结构，因此单点登录 Web 站点的任何更新仅影响正在同一服务器上运行的那些数据源产品。

数据源支持

CA 单点登录支持以下所有数据源：

- CA Infrastructure Management Data Aggregator
- CA Network Flow Analysis
- CA Application Delivery Analysis
- CA Unified Communications Monitor

在设计上，单点登录配置工具运行在 Linux 系统上。然而，您也能在安装数据源的 Windows 服务器上部署它。如果您从 Windows 服务器上启动配置工具，请在该服务器上以管理员身份登录。

通过使用“远程值”选项，您也可以在 Linux 上运行配置工具，并将配置说明发送到运行在 Windows 上的数据源。

在 Linux 上，配置工具安装于以下目录位置中：
`[安装目录]/CA/PerformanceCenter`

在安装数据源的 Windows 服务器上，配置工具安装于以下目录中：
`[InstallationDirectory]\Portal\SSO\bin\SsoConfig.exe`

单点登录配置工具

单点登录配置工具是一种命令行应用程序，允许管理员调整单点登录 Web 站点的设置和关联的 CA 数据源产品。

注意：配置工具的“远程值”选项会将设置传播到每个注册数据源。使用“本地覆盖”选项来覆盖选定服务器上的传播设置。

在设计上，单点登录配置工具运行在 Linux 系统上。然而，您也能在安装数据源的 Windows 服务器上部署它。如果您从 Windows 服务器上启动配置工具，请在该服务器上以管理员身份登录。

使用单点登录配置工具可以执行以下任务：

- 配置数据源产品以使用 LDAP 身份验证。

  每个产品的所有 LDAP 设置都使用该工具进行更新。也可以测试当前的 LDAP 配置以验证设置。

- 配置数据源产品以使用 SAML 2.0 身份验证。

  除使用配置工具之外，管理员还必须对身份提供程序采取一些措施，才可设置 SAML 身份验证。

- 更新每个产品引用的单点登录虚拟目录。

  如果添加了加密方案或更改了单点登录虚拟目录，请使用该工具同步数据源产品。例如，修改的服务器上的数据源需要有关重定向未成功进行身份验证的用户的位置的说明。

- 允许使用 HTTPS 在运行 CA 软件产品的服务器之间进行通信。

  该更改会影响单点登录 URL 方案和端口。通过单点登录配置工具，管理员可以在所有所需的数据源产品中轻松更新这些值。

备份单点登录配置文件

在您使用配置工具更改设置时，您的设置将在配置文件中加以保存。请定期创建这些文件的备份副本，以避免丢失单点登录设置。使用 rsync 或另一首选方式（如脚本）来自动备份这些文件或在升级前进行备份。

将下列文件添加到您的备份程序中：

InstallationDirectory/CA/PerformanceCenter/sso/start.ini
InstallationDirectory/CA/PerformanceCenter/PC/start.ini

还要备份以下目录：

InstallationDirectory/CA/PerformanceCenter/sso/webapps/sso/configuration
InstallationDirectory/CA/PerformanceCenter/sso/etc
InstallationDirectory/CA/PerformanceCenter/sso/conf
InstallationDirectory/CA/PerformanceCenter/PC/etc
InstallationDirectory/CA/PerformanceCenter/PC/conf

注意：默认安装目录为 opt/CA。

更新单点登录 Web 站点设置

通过单点登录配置工具，可以更改单点登录 Web 站点的默认设置。例如，可以更改单点登录 Web 站点的虚拟目录。虚拟目录需要使用加密方案才可在 CA 服务器之间进行通信。

可以更改在用户尝试登录时会影响单点登录行为的其他设置。有些参数也影响用户界面行为，以超时时段为例，它对处于不活动状态的用户响应结果是自动注销该用户。

重要说明！因为该软件的分布式体系结构，对单点登录网站的更新仅影响在同一服务器上运行的 CA 数据源产品。

遵循这些步骤:

1. 登录到安装了 CA Performance Center 或 CA 数据源产品的服务器。

   以 root 用户身份登录或使用“sudo”命令。

2. 在以下目录中运行“./SsoConfig”命令，以启动单点登录配置工具：

   [安装目录]/CA/PerformanceCenter

   系统会提示您选择一个选项。可用选项与在本地服务器上运行的 CA 应用程序相对应。

3. 选择设置时，根据需要使用以下命令：
   - q（退出）
   - b（返回上一级菜单）
   - u（更新）
   - r（重置）
4. 输入 1 以配置 CA Performance Center。

   系统会提示您选择一个选项。

```
SSO Configuration/CA Performance Center:
1. LDAP Authentication
2. SAML2 Authentication
3. Performance Center
4. Single Sign-On
5. Test LDAP
6. Export SAML2 Service Provider Metadata
Choose an option >
```

5. 对于单点登录输入 4。

   系统将提示您指定优先级。

   “优先级”参数仅适用于 CA Performance Center。
6. 输入以下选项之一：

   1. 远程值

   指的是只有管理员可以更改的设置。此类设置将传播到注册到此 CA Performance Center 实例的所有其他 CA 产品。仅当相应的“本地覆盖”值不存在时，才能使用“远程值”设置。

   2. 本地覆盖

   指的是可以针对所有产品更改的设置。如果“本地覆盖”值存在，其优先级将高于“远程值”和默认设置。

   系统将提示您选择要配置的属性。

7. 输入一个或多个以下属性。当出现提示时，输入 u 以更新值并提供新值：

1. 已启用匿名用户

指定当用户尝试登录到数据源界面时是否显示登录页。如果启用该参数，将需要“匿名用户 ID”参数的值。用户尝试登录时，看不到登录页。他们以与“匿名用户 ID”参数关联的用户身份登录。

当满足以下条件时，“已启用 Localhost 用户”参数优先级较高：

- 用户正在从单点登录服务器登录。
- “已启用 Localhost 用户”参数和“已启用匿名用户”参数都已启用。

默认值：已禁用。

注意：匿名用户登录的优先级高于 Windows 身份验证。

2. 匿名用户 ID

指定用于自动验证用户身份的用户名，即跳过登录页。只有启用“已启用匿名用户”参数时，才可使用该参数。选择以下值之一：

- **1**—默认管理员帐户的用户名 (admin)。
- **2**—默认用户帐户的用户名 (user)。
- 存在于 CA Performance Center 数据库中的其他用户名。

3. 已启用 Localhost 用户登录页

指定当用户从安装了单点登录的服务器登录时是否显示登录页。

如果启用该参数，将显示登录页，即使用户从单点登录服务器登录也会如此。

如果禁用该参数，则将应用下列规则：

- “已启用 Localhost 用户”参数必须处于启用状态。
- “Localhost 用户 ID”参数的值必须包含有效的产品用户名。该值用于使用户登录到软件界面，即跳过登录页。

默认值：已禁用。

4. 已启用 Localhost 用户

指定当用户从单点登录服务器登录时是否自动登录（跳过登录页）。如果启用该参数，将需要“Localhost 用户 ID”参数的值。

- 如果“已启用 Localhost 用户登录页”参数处于启用状态，则在用户不输入用户名或密码的情况下单击“登录”时将使用该参数。然后用户以与“Localhost 用户 ID”参数关联的用户身份登录到软件。
- 如果用户确实提供了用户名和密码，将使用这些凭据进行身份验证。
- 如果该参数处于启用状态，但“已启用 Localhost 用户登录页”参数处于禁用状态，用户将跳过登录页。用户会使用“Localhost 用户 ID”参数的值登录到界面。
- 如果用户从单点登录服务器登录，并且“已启用 Localhost 用户”和“已启用匿名用户”参数都处于启用状态，“已启用 Localhost 用户”参数优先级较高。

默认值：已禁用。

5. Localhost 用户 ID

指定当用户登录到单点登录服务器时自动对他们进行身份验证（即跳过登录页）所使用的用户 ID。只有启用“已启用 Localhost 用户”参数时，才可使用该参数。输入以下值之一：

1—默认管理员帐户的用户名 (admin)。

2—默认用户帐户的用户名 (user)。

6. Cookie 超时分钟数

指定在单点登录 Cookie 到期之前经过的分钟数。每次用户在数据源界面中执行操作时，Cookie 超时都会重置。如果超时到期，用户将注销并且必须重新进行身份验证。

默认值：20 分钟

7. 加密解密密钥

指定用于加密和解码单点登录 Cookie 的密钥。

8. 加密算法

指定用于加密和解码单点登录 Cookie 的加密算法。提供 DES 或 AES 作为值。

9. 失败睡眠秒数

指定单点登录应用程序在一次登录尝试失败之后等待的秒数。

10. 已启用保存我的信息

指定是否在登录页上显示“保存我的信息”复选框。“保存我的信息”设置确定，在 Cookie 超时到期时用户是否自动注销。

默认：已启用。

11. 保存我的信息超时天数

指定在登录页上选择了“保存我的信息”的用户在必须重新身份验证之前经过的天数。只有启用“已启用保存我的信息”参数时，才可使用该参数。值为 0 表示“保存我的信息”设置未到期；用户必须单击数据源产品界面中的“注销”链接。

12. 方案

指定数据源产品可用来访问单点登录应用程序的 URL 方案。如果正在使用 SSL，请提供“https:”作为值。

13. 端口

指定数据源产品可用来访问单点登录应用程序的 URL 端口。

14. 虚拟目录

指定单点登录的虚拟目录的名称。

默认值：SingleSignOn。

注意：如果更改前面任何参数的值，则不会替换默认值，但是新值的优先级较高。新值实际上是本地覆盖。

8. 已完成更改默认设置后，输入 b。
9. 返回到上一个选项集。
10. 再次输入 b 以返回到第一个选项集。
11. 输入 q 以关闭单点登录配置工具。

单点登录配置工具将关闭。

CA Performance Center 使用提供的新值将所有未经身份验证的用户定向到单点登录 Web 站点。

更新 CA Performance Center Web 站点设置

通过单点登录配置工具，可以更改 CA Performance Center Web 站点和 Web 服务的默认设置。例如，可以为 CA Performance Center Web 服务指定不同的主机或端口号。这些设置指导单点登录应用程序如何连接到 CA Performance Center。

遵循这些步骤:

1. 登录到安装了 CA Performance Center 或 CA 数据源产品的服务器。

   以 root 用户身份登录或使用“sudo”命令。

2. 在以下目录中运行“./SsoConfig”命令，以启动单点登录配置工具：

   ```
   [InstallationDirectory]/CA/PerformanceCenter
   ```

   系统会提示您选择一个选项。可用选项与在本地服务器上运行的 CA 应用程序相对应。

3. 选择设置时，根据需要使用以下命令：

   - q（退出）
   - b（返回上一级菜单）
   - u（更新）
   - r（重置）

4. 输入 1 以配置 CA Performance Center。

   系统会提示您选择配置选项。

   ```
   SSO Configuration/CA Performance Center:
   1. LDAP Authentication
   2. SAML2 Authentication
   3. Performance Center
   4. Single Sign-On
   5. Test LDAP
   6. Export SAML2 Service Provider Metadata
   Choose an option >
   ```

5. 为 Performance Center 输入 3。

   系统将提示您指定优先级。

   “优先级”参数仅适用于 CA Performance Center。

6. 输入以下选项之一：

   1. 远程值

   指的是只有管理员可以更改的设置。此类设置将传播到注册到此 CA Performance Center 实例的所有其他 CA 产品。仅当相应的“本地覆盖”值不存在时，才能使用“远程值”设置。

   2. 本地覆盖

   指的是可以针对所有产品更改的设置。如果“本地覆盖”值存在，其优先级将高于“远程值”和默认设置。

   系统将提示您选择要配置的属性。

7. 输入一个或多个以下属性。当出现提示时，输入 u 以更新值并提供新值：

   1. Web 服务方案

   指定单点登录应用程序可以用来访问 CA Performance Center Web 服务的 URL 方案。如果要使用 SSL 进行加密，请将该值更改为“https”。

   2. Web 服务主机

   指定单点登录应用程序可以在其上访问 CA Performance Center Web 服务的主机的 URL。

   3. Web 服务端口

   指定单点登录应用程序可以用来访问 CA Performance Center Web 服务的 URL 端口。

   4. Web 服务清单

   指定单点登录应用程序可以用来访问 CA Performance Center 清单 Web 服务的 URL 路径。

   5. Web 服务产品请求

   指定单点登录应用程序可以用来访问 CA Performance Center 产品请求 Web 服务的 URL 路径。

   6. Web 站点方案

   指定单点登录应用程序可以用来访问 CA Performance Center 的 URL 方案。如果已设置 SSL，请使用 https://。

   7. Web 站点主机

   指定单点登录应用程序可以用来访问 CA Performance Center 的 URL 主机。

8. Web 站点端口

指定单点登录应用程序可以用来访问 CA Performance Center 的 URL 端口。

9. Web 站点路径

指定单点登录应用程序可以用来访问 CA Performance Center 的 URL 路径。

10. 已启用 SMTP

指定是否启用简单邮件传输协议 (SMTP)，以允许 CA Performance Center 操作员以电子邮件方式发送报告和事件通知。

默认值：已禁用。

11. SMTP 服务器地址

是 SMTP 服务器的 IP 地址。

默认值：已禁用。

12. SMTP 端口：

指定用于 SMTP 请求的端口。

默认值：端口 25。

13. SMTP SSL

指定从 CA Performance Center 或其他 CA 数据源产品发送电子邮件时是否使用 SSL 加密。在启用该选项之前，请确认已在系统上正确设置了 SSL。

默认值：已禁用。

14. 电子邮件回复地址

指定用于 CA Performance Center 所生成电子邮件的回复地址。输入 u 以更新值，并提供电子邮件地址。使用格式 username@mydomain.com。

15. 电子邮件格式

指定用于 CA Performance Center 所发送电子邮件的格式。输入 u 以更新值，并且供 HTML 或文本。

16. SMTP 用户名

指定当电子邮件服务器查询 SMTP 请求时要使用的用户名。提供用户名，或提供空字符串以禁用客户端身份验证。

17. SMTP 密码

指定当电子邮件服务器查询 SMTP 请求时要使用的用户名。提供任何有效的密码。“SMTP 用户名”参数是必需的。

8. 已完成更改默认设置后，输入 b。

   返回到上一个选项集。

9. 再次输入 b 以返回到第一个选项集。

10. 输入 q 以退出。

    单点登录配置工具将关闭。

    CA Performance Center 使用提供的新值将所有用户定向到单点登录 Web 站点。

第 2 章： 设置 LDAP 身份验证

此部分包含以下主题：

LDAP 支持

单点登录提供了 LDAP 集成，允许操作员在您的环境中运行的轻型目录访问协议 (LDAP) 服务器上进行身份验证。经过身份验证后，可以将这些操作员映射到管理员可以指定的用户帐号：映射到预定义的用户帐号，或映射到自定义帐户。

通过单点登录配置工具，可以精确地指定单点登录服务器如何连接到 LDAP 服务器。还可以将各个 CA Performance Center 用户映射到支持其工作流的用户帐户，同时保护敏感数据。

注意：在单点登录配置工具中所做的更改仅影响新创建的 LDAP 用户。它们不会影响在 CA Performance Center 内注册的现有 LDAP 用户。

通过单点登录配置工具中提供的 LDAP 参数，可以将 CA Infrastructure Management 和所有注册的数据源集成到现有的身份验证方案。例如，LDAP 服务器可以授权多组用户，这些用户将映射到 CA Performance Center 中的单个自定义用户帐户。实际帐户名称和 LDAP 组可以广泛地自定义。通过搜索范围参数，可以确定如何进行目录搜索。可以选择验证用户时考虑的用户帐户属性。

启用无需身份验证机制的 LDAP 身份验证

使用 Single Sign-On 配置工具可以指导注册的数据源使用相同的 LDAP 方案验证用户的身份。在 Single Sign-On 配置工具中，您可以提供使 CA 服务器能够安全连接到 LDAP 服务器的参数。使用配置工具，也可以将 LDAP 目录中的用户与 CA Performance Center 中的预定义或自定义用户帐户相关联。

如果您使用了身份验证机制 (p. 24)（如 GSSAPI），则启用 LDAP 身份验证的步骤会略有不同。如果没有身份验证机制，则必须使用服务帐户绑定到 LDAP 服务器。此帐户需具有读取和搜索 LDAP 服务器的权限。必须提供连接用户的完整 DN（可识别名称），同时启用“用户绑定”参数。

Single Sign-On 使用您为“连接用户”和“连接密码”参数提供的凭据，绑定到 LDAP 服务器。然后，根据您为“搜索字符串”参数提供的字符串执行目录搜索。搜索结果包括用户的 DN。Single Sign-On 使用此 DN 和密码再次绑定到 LDAP 服务器。

重要说明！如果没有使用身份验证机制，我们强烈建议您建立与 LDAP 服务器的 SSL 连接。否则，密码将以明文方式发送至 LDAP 服务器。

遵循这些步骤:

1. 登录到安装了 CA Performance Center 或 CA 数据源产品的服务器。

   以 root 用户身份登录或使用“sudo”命令。

2. 在以下目录中运行“./SsoConfig”命令，以启动 Single Sign-On 配置工具：

   InstallationDirectory/CA/PerformanceCenter

   系统会提示您选择一个选项。可用选项与在本地服务器上运行的 CA 应用程序相对应。

3. 选择设置时，根据需要使用以下命令：
   - q（退出）
   - b（返回上一级菜单）
   - u（更新）
   - r（重置）

4. 输入 1 以配置 CA Performance Center。

   系统会提示您选择一个选项。

5. 对于 LDAP 身份验证输入 1。

   系统将提示您指定优先级。

   “优先级”参数仅适用于 CA Performance Center。

6. 输入以下选项之一：

   1. 远程值

   指的是只有管理员可以更改的设置。此类设置将传播到注册到此 CA Performance Center 实例的所有其他 CA 产品。仅当相应的“本地覆盖”值不存在时，才能使用“远程值”设置。

   2. 本地覆盖

   指的是可以针对所有产品更改的设置。如果“本地覆盖”值存在，其优先级将高于“远程值”和默认设置。

   系统将提示您选择要配置的属性。

7. 输入一个或多个以下属性。当出现提示时，输入 u 以更新值并提供新值：

   1. 连接用户

   定义登录服务器用于连接 LDAP 服务器的用户 ID（在本示例中为服务帐户的用户 ID）。该 LDAP 用户名用于绑定到服务器。

   重要说明！如果没有使用验证机制（如 GSSAPI），此参数需使用具有 LDAP 服务器读取与搜索权限的服务帐户。

   2. 连接密码

   定义登录服务器用来连接 LDAP 服务器的密码。

   示例：如果登录服务器使用固定帐户，请按下例那样输入文本：

   ```
   SomePassword
   ```

   3. 搜索域

   标识 CA Single Sign-On 连接到的 LDAP 服务器和端口。还标识在验证用户帐户凭据时搜索在目录树中查找用户的位置。如果您在字符串中的服务器后面也不提供端口号，则使用端口 389。

   为搜索域使用以下格式：

   LDAP://*ldap 服务器*:*端口*/*搜索路径*

   注意：搜索路径是*必需的*。

4. 搜索字符串

指定用于查找用户正确记录所使用的条件。与“搜索范围”参数一起使用。如果仅允许某些 LDAP 用户登录，则可以使用该搜索字符串查找该记录中的多个属性。该参数的值可以包括任何有效的 LDAP 搜索条件。

示例：

```
(saMAccountName={0})
```

5. 搜索范围

指定用于查找用户正确记录所使用的条件。与搜索字符串参数一起使用。确定 LDAP 服务器对用户帐户执行的搜索范围。键入以下值之一：

onelevel

在搜索中包括当前目录。匹配当前目录中的对象，并阻止目录中更深层次的非预期匹配项。

subtree

在搜索中包括所有子目录。建议在用于多数安装中使用该值。

基本

将搜索限制到基对象。

6. 用户绑定

指定是否使用用户的可识别名称 (DN) 和密码进行附加身份验证步骤（绑定）以验证提供的凭据。

重要说明！ 如果您在步骤 1 和步骤 2 中输入了服务帐户，则必须将此参数设为“已启用”。

默认值：已禁用。

7. 加密

指定再次绑定到 LDAP 服务器时使用的身份验证机制。

默认：Simple。

接受值：Simple、GSSAPI、DIGEST-MD5。

8. 帐户用户

指定将缺少组成员身份的已验证 LDAP 用户映射到的 CA Performance Center 默认帐户。与帐户密码参数一起使用。如果某个有效用户与所有组定义均不匹配，该用户将使用为该参数指定的默认用户 ID 登录。

要允许所有用户使用他们自己的用户名登录，请输入：

- {saMAccountName}
- {saMAccountName} 或 {CN}

注意：帐户用户参数对应于该用户的目录条目中的字段。该值通常与您的搜索筛选匹配。

9. 帐户用户默认克隆

指定要克隆的用户帐户（如果已验证的 LDAP 用户不是为组参数指定的组的成员）。

示例：如果您希望此类用户拥有最小权限，请输入“user”。

注意：现有的用户帐户是必要的。

10. Group

用于为选定的用户帐户或帐户组确定默认帐户处理。

示例：要使组内的所有成员都能够使用管理员帐户登录，请输入：

```
<LDAPGroups><Group searchTag="memberOf" searchString="CN=SEC_All
Employees,CN=Users,DC=company,DC=local" user="{saMAccountName}"
passwd="" userClone="admin"/></LDAPGroups>
```

11. 超时

指定 CA Performance Center 等待的时间量，同时对 LDAP 服务器进行权限检查。在授权检查超时的时候，拒绝试图登录的用户进行访问。要查看错误，请打开 SSOService.log 文件。默认超时值为 10000。

8. 验证 LDAP 状态是否设为“已启用”。如果 LDAP 状态设成“禁用”，那么验证使用内部性能中心用户数据库。
9. 输入 q 以退出。

   配置工具将关闭。

配置示例

1. 连接用户：CN=********, OU=Role-Based, OU=North America, DC=ca, DC=com [服务帐户的完整 DN]
2. 连接密码：******* [服务帐户的密码]
3. 搜索域：LDAP://******.ca.com/DC=ca,DC=com
4. 搜索字符串：(sAMAccountName={0})
5. 搜索范围：Subtree
6. 用户绑定：已启用
7. 加密：false
8. 帐户用户：{sAMAccountName}
9. 帐户用户默认克隆：user
10. 组：“All Employees”
11. Krb5ConfigFile: krb5.conf

使用 GSSAPI 加密与 LDAP 服务器的连接

CA Single Sign-On 支持使用 DIGEST-MD5 或 GSSAPI 加密的连接。使用指向目录服务器的加密连接时，不必使用服务帐户绑定到 LDAP 服务器（在“单点登录配置”工具中设置的 UserBind 参数）。

要使用 GSSAPI 加密，您必须更改配置文件的一些设置。

遵循这些步骤:

1. 登录到安装了 CA Performance Center 或 CA 数据源产品的服务器。

   以 root 用户身份登录或使用“sudo”命令。
2. 转到以下目录：
   `[安装目录]/webapps/sso/Configuration/`

3. 在该目录中打开要编辑的 krb5.conf 文件。
4. 设置以下所需参数：

```
[libdefaults]
        default_realm = CA.COM
[realms]
        CA.COM  = {
                kdc = EXAMPLE.CA.COM
                default_domain = CA.COM
}

[domain_realm]
       .CA.COM = CA.COM
}
```

其中：

[libdefaults]

包含 Kerberos V5 库的默认值。

default_realm

将子域和域名映射到 Kerberos 领域名。允许程序基于主机的完全限定域名确定其领域。在此示例中，默认领域为 CA.COM。

realms

包含有关 Kerberos 领域名的信息，其中描述了 Kerberos 服务器的位置并包括其他一些领域特定信息。

kdc

是支持身份验证服务的 Kerberos 密钥分发中心。例如 EXAMPLE.CA.COM。

default_domain

是默认 IP 域。例如 CA.COM。

注意：Active Directory 或 LDAP 管理员可能会为您提供或帮助您创建一个 krb5.conf 文件。

5. 保存更改。
6. 现在，请按照使用加密机制启用 LDAP 身份验证 (p. 26)中的步骤，对 CA 单点登录配置 LDAP 身份验证。

启用使用加密机制的 LDAP 身份验证

使用 Single Sign-On 配置工具可以指导注册的数据源使用相同的 LDAP 方案验证用户的身份。在 Single Sign-On 配置工具中，您可以提供使 CA 服务器能够安全连接到 LDAP 服务器的参数。在您使用 Digest-MD5 或 GSSAPI 加密与 LDAP 服务器的连接时，单个绑定操作 - 以您指定的用户身份 - 便会发生。

使用配置工具，也可以将 LDAP 目录中的用户与 CA Performance Center 中的预定义或自定义用户帐户相关联。

遵循这些步骤:

1. 登录到安装了 CA Performance Center 或 CA 数据源产品的服务器。

   以 root 用户身份登录或使用“sudo”命令。

2. 在以下目录中运行“./SsoConfig”命令，以启动 Single Sign-On 配置工具：

   InstallationDirectory/CA/PerformanceCenter

   系统会提示您选择一个选项。可用选项与在本地服务器上运行的 CA 应用程序相对应。

3. 选择设置时，根据需要使用以下命令：

   - q（退出）
   - b（返回上一级菜单）
   - u（更新）
   - r（重置）

4. 输入 1 以配置 CA Performance Center。

   系统会提示您选择一个选项。

5. 对于 LDAP 身份验证输入 1。

   系统将提示您指定优先级。

   “优先级”参数仅适用于 CA Performance Center。

6. 输入以下选项之一：

   1. 远程值

   指的是只有管理员可以更改的设置。此类设置将传播到注册到此 CA Performance Center 实例的所有其他 CA 产品。仅当相应的“本地覆盖”值不存在时，才能使用“远程值”设置。

   2. 本地覆盖

   指的是可以针对所有产品更改的设置。如果“本地覆盖”值存在，其优先级将高于“远程值”和默认设置。

   系统将提示您选择要配置的属性。

7. 输入一个或多个以下属性。当出现提示时，输入 u 以更新值并提供新值：

   1. 连接用户

   定义登录服务器用来连接 LDAP 服务器的用户 ID。该 LDAP 用户名用于绑定到服务器。对于使用身份验证机制（如 GSSAPI）的连接，通常不需要服务帐户。

   示例：如果登录服务器使用固定帐户，请按以下语法输入文本：

   ```
   CN=The User,cn=Users,dc=domain,dc=com
   ```

   或您可以输入以下值，因为连接将使用身份验证机制：

   ```
   {0}
   ```

   复杂配置需要用户主要名称来识别用户。提供“{0}”，并使用他们的电子邮件地址作为域名。例如：

   ```
   {0}@domain.com
   ```

   对于加密连接，LDAP 服务器通常不需要完全域名。

   注意：出于安全考虑，请不要使连接用户成为静态帐户。当绑定到服务器时，LDAP 身份验证仅检查密码。如果使用静态帐户，则 LDAP 树中的任何用户将都可以使用任何密码进行登录。

   2. 连接密码

   定义登录服务器用来连接 LDAP 服务器的密码。

   示例：如果登录服务器使用固定帐户，请按下例那样输入文本：

   ```
   SomePassword
   ```

   或您可以输入以下值，因为连接将使用身份验证机制：

   ```
   {1}
   ```

3. 搜索域

标识 CA Single Sign-On 连接到的 LDAP 服务器和端口。还标识在验证用户帐户凭据时搜索在目录树中查找用户的位置。如果您在字符串中的服务器后面也不提供端口号，则使用端口 389。

为搜索域使用以下格式：

LDAP://*ldap 服务器*:*端口*/*搜索路径*

注意：搜索路径是*必需的*。

4. 搜索字符串

指定用于在该目录中查找正确用户的条件。与“搜索范围”参数一起使用。如果仅允许某些 LDAP 用户登录，则可以使用该搜索字符串在一个记录中搜索多个属性。该参数的值可以包括任何有效的 LDAP 搜索条件。

示例：

```
(saMAccountName={0})
```

5. 搜索范围

指定用于查找用户正确记录所使用的条件。与搜索字符串参数一起使用。确定 LDAP 服务器对用户帐户执行的搜索范围。键入以下值之一：

onelevel

在搜索中包括当前目录。匹配当前目录中的对象，并阻止目录中更深层次的非预期匹配项。

subtree

在搜索中包括所有子目录。建议在用于多数安装中使用该值。

基本

将搜索限制到基对象。

6. 用户绑定

指定是否使用用户的可识别名称 (DN) 和密码进行附加身份验证步骤（绑定）以验证提供的凭据。

默认值：已禁用。此值对于加密连接可接受。

7. 加密

指定再次绑定到 LDAP 服务器时使用的身份验证机制。

在这种情况下（也就是说，使用身份验证机制），根据您的 LDAP 服务器的机制，输入“GSSAPI”或“DIGEST-MD5”。

默认：Simple。

接受值：Simple、GSSAPI、DIGEST-MD5。

8. 帐户用户

指定将缺少组成员身份的已验证 LDAP 用户映射到的 CA Performance Center 默认帐户。与帐户密码参数一起使用。如果某个有效用户与所有组定义均不匹配，该用户将使用为该参数指定的默认用户 ID 登录。

要允许所有用户使用他们自己的用户名登录，请输入：

- {saMAccountName}
- {saMAccountName} 或 {CN}

注意：帐户用户参数对应于该用户的目录条目中的字段。该值通常与您的搜索筛选匹配。

9. 帐户用户默认克隆

指定要克隆的用户帐户，如果已验证 LDAP 用户不是为组参数指定的组的成员。

示例：如果您希望此类用户拥有最小权限，请输入“user”。

注意：现有的用户帐户是必要的。

10. Group

用于为选定的用户帐户或帐户组确定默认帐户处理。

示例：要使组内的所有成员都能够使用管理员帐户登录，请输入：

```
<LDAPGroups><Group searchTag="memberOf" searchString="CN=SEC_All
Employees,CN=Users,DC=company,DC=local" user="{saMAccountName}"
passwd="" userClone="admin"/></LDAPGroups>
```

11. 超时

指定 CA Performance Center 等待的时间量，同时对 LDAP 服务器进行权限检查。在授权检查超时的时候，拒绝试图登录的用户进行访问。要查看错误，请打开 SSOService.log 文件。默认超时值为 10000。

8. 验证 LDAP 状态是否设为“已启用”。如果 LDAP 状态设成“禁用”，那么验证使用内部性能中心用户数据库。
9. 输入 q 以退出。

   配置工具将关闭。

配置示例

1. SSO 配置/CA Performance Center/LDAP 身份验证/远程值：
2. 连接用户：{0}
3. 连接密码：{1}
4. 搜索域：LDAP://******.ca.com/DC=ca,DC=com
5. 搜索字符串：(sAMAccountName={0})

6. 搜索范围：Subtree
7. 用户绑定：已禁用
8. 加密：DIGEST-MD5
9. 帐户用户：{sAMAccountName}
10. 帐户用户默认克隆：user
11. 组：“All Employees”
12. Krb5ConfigFile: krb5.conf

详细信息：

使用 GSSAPI 加密与 LDAP 服务器的连接 (p. 24)

启用 LDAPS 身份验证

使用单点登录配置工具指示注册数据源将在 SSL 上的 LDAP (LDAPS) 用于安全用户身份验证。默认情况下，LDAP 通信量的传输安全不能保证。通过从认证机构 (CA) 安装证书来启用 LDAPS。使用 CA Single Sign-On，您必须将证书导入 Java 信任的密钥存储库。

在 Single Sign-On 配置工具中，您可以提供使 CA 服务器能够安全连接到 LDAP 服务器的参数。使用配置工具，也可以将 LDAP 目录中的用户与 CA Performance Center 中的预定义或自定义用户帐户相关联。

遵循这些步骤:

1. 登录到安装了 CA Performance Center 或 CA 数据源产品的服务器。

   以 root 用户身份登录或使用“sudo”命令。
2. 按照名为导入 LDAP 证书 (p. 34)主题中的说明获取您的证书并将其导入 Java 密钥存储库。
3. 在以下目录中运行“./SsoConfig”命令，以启动 Single Sign-On 配置工具：

   InstallationDirectory/CA/PerformanceCenter

   系统会提示您选择一个选项。可用选项与在本地服务器上运行的 CA 应用程序相对应。

4. 选择设置时，根据需要使用以下命令：
   - q（退出）
   - b（返回上一级菜单）
   - u（更新）
   - r（重置）
5. 输入 1 以配置 CA Performance Center。

   系统会提示您选择一个选项。
6. 对于 LDAP 身份验证输入 1。

   系统将提示您指定优先级。

   “优先级”参数仅适用于 CA Performance Center。
7. 输入以下选项之一：

   1. 远程值

   指的是只有管理员可以更改的设置。此类设置将传播到注册到此 CA Performance Center 实例的所有其他 CA 产品。仅当相应的“本地覆盖”值不存在时，才能使用“远程值”设置。

   2. 本地覆盖

   指的是可以针对所有产品更改的设置。如果“本地覆盖”值存在，其优先级将高于“远程值”和默认设置。

   系统将提示您选择要配置的属性。
8. 输入一个或多个以下属性。当出现提示时，输入 u 以更新值并提供新值：

   1. 连接用户

   定义登录服务器用来连接 LDAP 服务器的用户 ID。该 LDAP 用户名用于绑定到服务器。对于使用身份验证机制（如 GSSAPI）的连接，通常不需要服务帐户。

   示例：如果登录服务器使用固定帐户，请按以下语法输入文本：

   ```
   CN=The User,cn=Users,dc=domain,dc=com
   ```

   或您可以输入以下值，因为连接将使用身份验证机制：

   ```
   {0}
   ```

复杂配置需要用户主要名称来识别用户。提供“{0}”，并使用他们的电子邮件地址作为域名。例如：

```
{0}@domain.com
```

对于加密连接，LDAP 服务器通常不需要完全域名。

注意：出于安全考虑，请不要使连接用户成为静态帐户。当绑定到服务器时，LDAP 身份验证仅检查密码。如果使用静态帐户，则 LDAP 树中的任何用户将都可以使用任何密码进行登录。

2. 连接密码

定义登录服务器用来连接 LDAP 服务器的密码。

示例：如果登录服务器使用固定帐户，请按下例那样输入文本：

```
SomePassword
```

或您可以输入以下值，因为连接将使用身份验证机制：

```
{1}
```

3. 搜索域

标识 CA Single Sign-On 连接到的 LDAP 服务器和端口。还标识在验证用户帐户凭据时搜索在目录树中查找用户的位置。如果您在字符串中的服务器后面也不提供端口号，则使用端口 389。

为搜索域使用以下格式：
LDAPS://*ldap 服务器*:*端口*/*搜索路径*

注意：搜索路径是*必需的*。

要建立与 LDAP 服务器的 SSL 连接，请使用 636 或其他 SSL 连接端口与您的 LDAP 服务器连接：

```
LDAPS://LDAP 服务器:636/OU=Users,OU=North
America,DC=ca,DC=com
```

4. 搜索字符串

指定用于在该目录中查找正确用户的条件。与“搜索范围”参数一起使用。如果仅允许某些 LDAP 用户登录，则可以使用该搜索字符串在一个记录中搜索多个属性。该参数的值可以包括任何有效的 LDAP 搜索条件。

示例：

```
(saMAccountName={0})
```

5. 搜索范围

指定用于查找用户正确记录所使用的条件。与搜索字符串参数一起使用。确定 LDAP 服务器对用户帐户执行的搜索范围。键入以下值之一：

onelevel

在搜索中包括当前目录。匹配当前目录中的对象，并阻止目录中更深层次的非预期匹配项。

subtree

在搜索中包括所有子目录。建议在用于多数安装中使用该值。

基本

将搜索限制到基对象。

6. 用户绑定

指定是否使用用户的可识别名称 (DN) 和密码进行附加身份验证步骤（绑定）以验证提供的凭据。

默认值：已禁用。此值对于加密连接可接受。

7. 加密

（可选）指定再次绑定到 LDAP 服务器时使用的身份验证机制。

LDAPS 可接受默认设置（简单身份验证）。

8. 帐户用户

指定将缺少组成员身份的已验证 LDAP 用户映射到的 CA Performance Center 默认帐户。与帐户密码参数一起使用。如果某个有效用户与所有组定义均不匹配，该用户将使用为该参数指定的默认用户 ID 登录。

要允许所有用户使用他们自己的用户名登录，请输入：

- {saMAccountName}
- {saMAccountName} 或 {CN}

注意：帐户用户参数对应于该用户的目录条目中的字段。该值通常与您的搜索筛选匹配。

9. 帐户用户默认克隆

指定要克隆的用户帐户，如果已验证 LDAP 用户不是为组参数指定的组的成员。

示例：如果您希望此类用户拥有最小权限，请输入“user”。

注意：现有的用户帐户是必要的。

10. Group

用于为选定的用户帐户或帐户组确定默认帐户处理。

示例：要使组内的所有成员都能够使用管理员帐户登录，请输入：

```
<LDAPGroups><Group searchTag="memberOf" searchString="CN=SEC_All
Employees,CN=Users,DC=company,DC=local" user="{saMAccountName}"
passwd="" userClone="admin"/></LDAPGroups>
```

9. 输入 q 以退出。

   配置工具将关闭。

配置示例

1. SSO Configuration/CA Performance Center/LDAP Authentication/Remote Value
2. 连接用户：{0}
3. 连接密码：{1}
4. 搜索域：LDAPS://******.ca.com:636/OU=Users,OU=North America,DC=ca,DC=com
5. 搜索字符串：(sAMAccountName={0})
6. 搜索范围：Subtree
7. 用户绑定：已禁用
8. 加密：简单的
9. 帐户用户：{sAMAccountName}
10. 帐户用户默认克隆：user
11. 组：“All Employees”
12. Krb5ConfigFile: krb5.conf

导入 LDAP 证书

要通过 LDAPS 运行，您必须将 LDAP 证书导入 Java 密钥库。

如果还没有 SSL 证书，您可以使用 keytool 命令生成一个。此过程解释如何从 CA 导入证书并且将其安装在密钥库中。

遵循这些步骤:

1. 从 LDAP 服务器管理员获得证书。

2. 使用下列命令将证书导入 Java 信任的证书密钥库：

   ```
   keytool -importcert -keystore installDirectory/jre/
   lib/security/cacerts -storepass cacertspasswd -alias
   alias -file filename.cer
   ```

   keystore

   密钥库文件 (.ks) 的位置

   cacertspasswd

   为 cacerts keystore 指定密码。

   默认值：changeit

   filename.cer

   证书的文件名。

3. 对 cacerts 文件进行备份。
4. （可选）为提高安全性，使用以下命令更改 java 信任的证书 keystore 的密码：

   ```
   keytool -storepasswd -keystore installDirectory/
   jre/lib/security/cacerts
   ```

   系统会提示您提供现有密码和新密码。

5. 确认您导入的证书可用。使用以下命令：

   ```
   keytool -list -keystore installDirectory/jre/
   lib/security/cacerts
   ```

   重要说明！要启用 Web 服务，证书必须位于 cacerts 密钥库中。否则，您会在日志中看到报告 PKIX 未找到证书的错误。

验证 LDAP 设置

您可以使用单点登录配置工具测试您已经提供的 LDAP 设置。您可以验证 LDAP 身份验证是否设置正确。LDAP 测试脚本提示您指定用户名和密码组合，以便使用 LDAP 身份验证的当前设置进行测试。如果您尚未使用配置工具来更改 LDAP 身份验证设置，将使用默认值。

遵循这些步骤:

1. 登录到其中安装了 CA Performance Center 或支持的数据源产品的服务器。

   以 root 用户身份登录或使用“sudo”命令。

2. 在以下目录中运行“./SsoConfig”命令，以启动单点登录配置工具：

   ```
   [InstallationDirectory]/CA/PerformanceCenter
   ```

   系统会提示您选择一个选项。可用选项与在本地服务器上运行的 CA 应用程序相对应。

3. 选择设置时，根据需要使用以下命令：

   - q（退出）
   - b（返回上一级菜单）
   - u（更新）
   - r（重置）

4. 输入 1 以配置 CA Performance Center。

   系统会提示您选择一个选项。

5. 为“测试 LDAP”选项输入 5。

   提示将要求您输入用户名。

6. 输入您知道的可以使用 LDAP 进行身份验证的用户名和密码。

   设置 LDAP 身份验证以连接至 LDAP 服务器并验证用户帐户时，单点登录会尝试使用您提供的参数。如果测试成功，会记录无数个步骤。

   将显示一条消息，报告身份验证是否成功。

7. 输入 q 以退出。

第 3 章： 设置 SAML 2.0 支持

此部分包含以下主题：

关于 SAML 2.0

安全断言标记语言 (*SAML*) 是基于 XML 的安全协议。基本概念涉及关于请求对安全域的访问权限的对象（人或计算机）的安全断言的交换。断言包括对象是否可以访问特定资源，以及是否使用外部数据源（如策略存储）。

基于 SAML 的身份验证通常在联合环境中使用，如需要在公司网络中包含额外安全层的基于云的服务。但是，任何 SAML 实施均涉及至少三个组件角色：

依赖方

使用存储在另一个服务器上的身份信息来允许已授权的用户获得访问系统的权限。也称为“服务提供商”。当单点登录配置为使用 SAML 进行身份验证时，CA Performance Center 具有该角色。

声明方

存储身份或安全信息，并且当出于身份验证目的而请求这些信息时提供信息。针对该组件的 SAML 术语是*身份提供商*或 *IdP*。例如，CA SiteMinder 服务器具有该角色。

主题

是与 IdP 所存储的身份信息关联的用户（或计算机）。

单点登录中的 SAML 2.0 支持

CA 单点登录支持使用安全声明标记语言 (SAML) 版本 2.0 来进行身份验证。单点登录服务可以接受和解码 SAML 2.0 内标识，并且可以呈现这些内标识，以便对符合 SAML 标准的代理进行身份验证。

SAML 2.0 的单点登录支持包括对单个注销的支持。通过这种支持，登录到多个用户界面的用户可以同时注销所有这些界面。例如，登录到 CA Performance Center 并稍后深入查看 CA Network Flow Analysis 中流数据的用户可以注销一个界面，然后会自动注销另一个界面。

单点登录使用基于标准的 SAML 2.0 库。因此，它可能支持更多依赖 SAML 2.0 标准的产品。不过，以下 CA 产品是我们使用 CA 单点登录经过测试后的唯一身份提供商：

- CA SiteMinder Federation Manager
- CA Arcot A-OK™ On-Demand

在 SAML 环境中，您可以从多个身份验证方法中进行选择。CA Performance Center 用户可以使用单点登录中的典型（“产品”）身份验证方法来登录，或者可以使用 SAML 内标识。默认情况下为所有活动用户帐户启用产品方式。用户使用 CA 单点登录的标准 URL 来访问 CA Performance Center 用户界面。

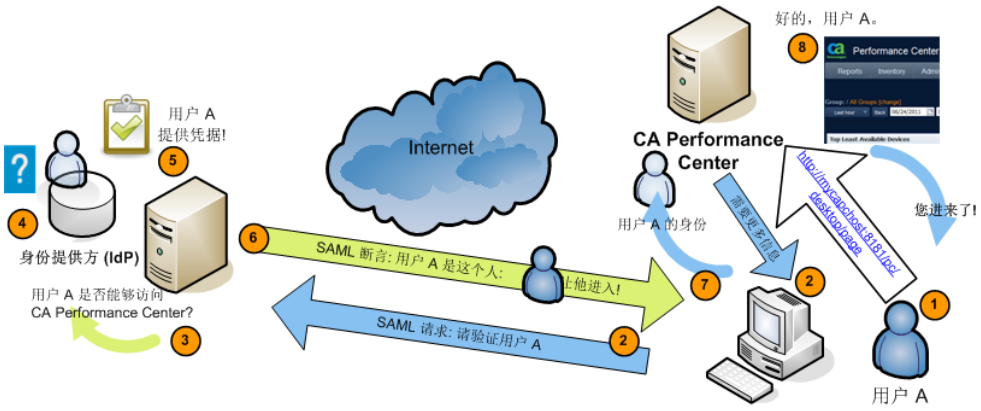
要使用户能够使用 SAML 2.0 进行身份验证，管理员必须使用配置工具更改某些单点登录设置。管理员还必须为所有用户帐户以及支持 SAML 2.0 的所有注册数据源启用外部身份验证。

并非所有 CA 数据源产品都支持 SAML 2.0。如果为单点登录中的外部身份验证配置 SAML 2.0，并且注册缺少 SAML 支持的数据源，则 CA Performance Center 用户在深入查看该数据源时必须重新进行身份验证。

SAML 2.0 的单点登录支持的工作方式

使用单点登录的通常 CA Performance Center 身份验证过程不同于利用 SAML 2.0 支持的身份验证。使用 SAML 2.0 身份验证，用户不会看到 CA Performance Center 登录页。相反，他们会重定向到 IdP 提供的界面。对于所有其他支持的身份验证方法，单点登录提供登录页。

下图说明使用单点登录、CA Performance Center 以及支持 SAML 2.0 标准的 IdP（如 CA SiteMinder）的 SAML 2.0 身份验证过程：



以下常规过程说明 CA Performance Center 如何支持 SAML 2.0 身份验证。特定于实施的选项（如数字签名证书和传输绑定）已省略：

1. 用户尝试访问 CA Performance Center，例如通过导航至 http://mycapchost:8181/pc/desktop/page。
2. CA Performance Center 以来自身份提供商 (IdP) 的 SAML 身份验证请求作为响应。
3. 浏览器处理请求，并联系在 IdP 服务器上运行的身份验证软件。
4. IdP 确定用户是否具有现有的登录安全性上下文－无论用户是否已登录。
5. 如果用户未登录，IdP 将使用特定于实施的方式对用户进行身份验证。

   例如，IdP 可能与浏览器交互以要求用户提供凭据。身份验证的此阶段与 CA 单点登录无关。
6. IdP 构建表示用户登录安全性上下文的 SAML 声明并将其发送到浏览器。

   声明包括必要属性 subjectNameId 和可选属性 ClonedUser。

   subjectNameId 的值对应于授权用户。

   您可以将克隆用户帐号的名称包含在声明中。该属性定义已授权 SAML 用户映射到的用户帐户。
7. 浏览器将 SAML 声明发送到 CA Performance Center。
8. CA Performance Center 获得声明并对其进行处理。
9. 如果声明有效，CA Performance Center 将为用户建立会话。浏览器将重定向到目标页面，即用户的主显示板页面。

如何设置 SAML 身份验证

要在单点登录中启用 SAML 2.0 身份验证，管理员必须执行以下过程：

1. 遵循特定于身份提供商 (IdP) 的指导，创建用于在 IdP 和单点登录之间建立协议的元数据文件。

   有关详细信息，请参阅准备 IdP 协议 (p. 40)。

2. （可选）创建属性文件，对 IdP 和运行 CA 软件的服务器之间的通信启用数字签名和加密。

   有关详细信息，请参阅准备安全属性文件 (p. 41)。

3. 使用单点登录配置工具设置 SAML 身份验证的参数。

   有关详细信息，请参阅在单点登录中配置 SAML 支持 (p. 42)。

4. 在 IdP 服务器上设置参数。例如，将支持 SAML 的所有数据源产品网站添加到信任站点列表中。

   有关详细信息，请参阅配置 IdP (p. 45)。

5. 更新 CA Performance Center 管理中的用户帐户来添加说明以使用外部身份验证。

   有关详细信息，请参阅完成 SAML 设置 (p. 46)。

准备 IdP 协议

需要 XML 格式的元数据文件来建立 IdP 和服务提供商之间的协议。在这种情况下，CA Performance Center 和支持 SAML 2.0 的所有注册数据源需要该协议。元数据文件介绍了 IdP 并包含有关它支持的配置文件的信息。该文件还包含它需要从服务提供商获取的服务的有关数据。

单点登录可以导入该文件以设置与 IdP 的关系。

某些类型的 IdP（如 CA SiteMinder）可提供实用工具来帮助您创建这些文件并将其导出。或者，它们基于您设置的参数自动创建协议。

请参考 IdP 文档来执行该任务。

准备安全属性文件

如果计划对 CA Performance Center 和 IdP 之间的通信使用加密和数字证书，则需要属性文件。在此文件中，您可指定要用于签名和加密的证书，并指定其他参数以启用加密。

SAML 属性文件保存在单点登录主目录中：
`/opt/CA/PerformanceCenter/sso/webapps/sso`

例如，需要如下文件：
`/opt/CA/PerformanceCenter/sso/webapps/sso/configuration/saml.properties`

属性文件必须包括以下参数：

- 签名证书的目录位置和文件名。
- 用于访问证书的验证证书别名和密码。
- CA Performance Center 服务器的主机名。
- 从 IdP 导出的协议的目录位置和文件名。
- IdP 上设置的超时时段的长度。值必须与单点登录中的“SAML2 IdP 会话超时”参数匹配。

下面是一个语法示例：

```
# Location of the certificate used for signing SAML documents
saml.sp.certificate.location=/opt/CA/saml2configuration/[Certificate filename]
saml.sp.certificate.password=[password]
saml.sp.certificate.alias=[alias]

saml.sp.metadata.hostname=[Full Hostname of CA Performance Center server]
saml.sp.metadata.entityID=[Name of the CA Performance Center server without IP domain]
saml.sp.metadata.organizationName=[Name of your organization]
saml.sp.metadata.contactPerson=[First and last name of administrator]
saml.sp.metadata.email=[Email address of contact person]

# Location of the metadata file for the Login Site
saml.idp.metadata.file=/opt/CA/saml2configuration/[Filename].xml
# Session timeout with the IdP in minutes. Use this value for auto-reauthentication and logout requests
saml.idp.sessionTimeout=[Length of timeout period in minutes]
```

每次修改 saml.properties 文件时，请重新导出元数据文件（该文件建立与 IdP 的协议）。有关详细信息，请参阅在单点登录中配置 SAML 2.0 支持 (p. 42)。您还必须重新启动单点登录。

在单点登录中配置 SAML 2.0 支持

CA Performance Center 管理员必须使用单点登录配置工具设置 SAML 身份验证的参数。在其中安装了数据源并且其用户将使用 SAML 2.0 进行身份验证的所有服务器上采取这些步骤。

注意：可以同时使用多个身份验证方案。例如，当 CA Infrastructure Management 的用户使用 SAML 2.0 时，CA Network Flow Analysis 数据源的用户可以使用 LDAP 来登录。

遵循这些步骤:

1. 登录到安装了 CA Performance Center 或 CA 数据源产品的服务器。

   以 root 用户身份登录或使用“sudo”命令。

2. 在以下目录中运行“./SsoConfig”命令，以启动单点登录配置工具：

   ```
   [InstallationDirectory]/CA/PerformanceCenter
   ```

   系统会提示您选择一个选项。可用选项与在本地服务器上运行的 CA 应用程序相对应。

3. 选择设置时，根据需要使用以下命令：

   - q（退出）
   - b（返回上一级菜单）
   - u（更新）
   - r（重置）

4. 输入与想要配置的数据源对应的值。例如，输入 1 来配置 CA Performance Center。

   系统会提示您选择一个选项。

5. 为 SAML 身份验证输入 2。

   系统将提示您指定优先级。

   “优先级”参数仅适用于 CA Performance Center。

6. 输入以下选项之一：

   1. 远程值

   指的是只有管理员可以更改的设置。此类设置将传播到注册到此 CA Performance Center 实例的所有其他 CA 产品。仅当相应的“本地覆盖”值不存在时，才能使用“远程值”设置。

   2. 本地覆盖

   指的是可以针对所有产品更改的设置。如果“本地覆盖”值存在，其优先级将高于“远程值”和默认设置。

   系统将提示您选择要配置的属性。

   要为 SAML2 属性提供值，请输入 u 以更新值，然后输入新值。

7. 输入 1 以选择“启用 SAML2 身份验证”参数。

   系统会提示您选择一个选项。

8. 输入 u 以更改值，输入 1 以启用 SAML 2.0 身份验证。

9. 输入 2 以设置“克隆默认用户帐户”参数。

   2. 克隆默认用户帐户

   定义已授权 SAML 用户映射到的用户帐户。与您指定的用户帐户关联的角色和产品权限将应用于成功进行身份验证的所有用户。

   默认值：空白。

   示例：如果希望所有用户使用用户级别权限登录，请输入“user”。

   注意：现有的用户帐户是必要的。

   协议建立之后，在 IdP 上配置的用户帐户将发送至 CA Performance Center。帐户将显示在“管理用户管理”页面上的用户列表中，您可以在其中编辑帐户。

10. 输入 3 以启用安全参数。

    3. 已启用 SAML2 签名和加密

    对 CA Performance Center 和 IdP 之间的通信启用安全和加密。

    默认值：已禁用

    系统会提示您选择一个选项。

11. 输入 u 以更改值，输入 1 以启用该设置。

    注意：该设置必须与 IdP 上的设置相匹配。

12. 输入 4 以启用自动重新身份验证。

    4. SAML2 自动重新身份验证

    指定是否要求用户在超过超时时段之后重新身份验证。启用该参数以允许 IdP 执行被动重新身份验证（“自动重新身份验证”），而不需要用户进行交互。

    下一个参数允许您设置超时时段的持续时间。

    默认值：已禁用。

13. 输入 u 以更改值，输入 1 以启用该设置。

14. 输入 5 以设置重新身份验证超时时段。

    5. 自动重新身份验证时段

    设置在执行被动重新身份验证之前经过的时长。如果“SAML2 自动重新身份验证”参数已禁用，将忽略该参数。

    值：必须小于“IdP 会话超时”参数的值。

    默认值：无。

15. 输入 u 以更改值，并输入新值。

16. 输入 6 以设置身份提供商的会话的超时时段。

    6. IdP 会话超时

    设置在 CA Performance Center 和身份提供商之间建立的会话自动关闭之前经过的时长。例如，输入“10”可设置 10 分钟的超时。

    该值必须大于为“自动重新身份验证持续时间”参数指定的值。否则，不会存在会话来执行重新身份验证。此外，该值还必须与安全属性文件中为“saml.idp.sessionTimeout”参数设置的值相匹配。有关详细信息，请参阅准备安全属性文件 (p. 41)。

    默认值：无。

17. 输入 u 以更改值，并输入新值。

18. 输入 b 两次以回到初始提示。

19. 输入 6 以导出与 IdP 建立协议的元数据文件。

    元数据文件向身份提供商提供在对用户进行身份验证时要使用的参数。

    系统将要求您提供目录路径和文件名。

20. 输入文件名。例如，输入以下内容：

    ```
    /tmp/CAPCMetadata.xml
    ```

    基于您在配置工具中所选的设置自动生成文件。

    如果导出操作成功，您将会看到 XML 的打印输出。如果操作失败，您将会看到一条错误消息。

21. 输入 q 以退出。

    配置工具将关闭。

配置 IdP

要开始在 CA Performance Center 中使用 SAML 2.0 来进行用户身份验证，请在身份提供商 (IdP) 上设置一些参数。任何支持 SAML 2.0 标准的 IdP 应当都可以使用，但是 CA 仅对 CA SiteMinder 进行了测试。

您可以手动配置 IdP，或者可以从单点登录服务器导入 IdP 协议。

手动配置 IdP

遵循这些步骤:

1. 在 IdP 上启用 SAML2 身份验证模式。
2. 为声明使用者服务提供 URL，该服务在安装有单点登录的服务器上运行。例如：

   ```
   http://MyServerName:8381/sso/saml2/UserAssertionService
   ```

   其中 8381 是单点登录使用的端口。
3. 将绑定方式设置为“HTTP-重定向”。

   注意：HTTP 重定向是单点登录支持的唯一绑定方式。
4. 为单个注销服务提供 URL。

   注销服务和响应位置都是必须的。这些服务在安装了单点登录的服务器上运行。

   请使用以下示例：

   ```
   http://MyServerName:8381/sso/saml2/LogoutService
   http://MyServerName:8381/sso/saml2/LogoutServiceResponse
   ```
5. 将支持 SAML 2.0 的所有数据源产品网站添加到信任站点列表中。

   此步骤可涉及将这些网站添加到联合合作伙伴关系实体列表中。
6. （*可选*）验证数字签名和加密设置。您还必须在单点登录中配置这些设置。

导入 IdP 协议文件

遵循这些步骤:

1. 从位于单点登录服务器上的 IdP 协议文件位置导入 IdP 协议文件。

   在使用单点登录配置工具完成其他设置步骤之后导出该文件。有关详细信息，请参阅在单点登录中配置 SAML 支持 (p. 42)。

2. 将支持 SAML 2.0 的所有数据源产品网站添加到信任站点列表中。

   此步骤可涉及将这些网站添加到联合合作伙伴关系实体列表中。

3. （*可选*）验证数字签名和加密设置。您还必须在单点登录中配置这些设置。

故障排除

问题：

配置 SAML 之后会显示以下错误消息：

```
RelayState is either null or a blank string. RelayState must be
set for SSO to work correctly.

Invalid syntax, RelayState=<value>

RelayState does not have parameter SsoRedirectUrl,
RelayState=<value>
```

原因：

一些 IdP 不返回 CA Performance Center 在身份验证期间发送给 IdP 的 RelayState= 值。

解决办法：

手动为您的 IdP 配置 RelayState。使用以下语法：

```
SsoProductCode=pc&SsoRedirectUrl=http://[assign the value for
CAPC in your book]:8181/pc/desktop/page
```

注意：为实现安全通信，请将 http: 替换为 https:，并替换端口号。

完成 SAML 2.0 设置

要启用 SAML 2.0 身份验证，请编辑用户帐户以使用外部身份验证。默认情况下，CA Performance Center 中的新用户帐户将被设置为使用 Performance Center 身份验证。管理员必须更新使用 SAML 2.0 进行身份验证的所有操作员的帐户。

在 SAML2.0 配置期间，您指定一个要在 IdP 中“克隆”的现有 CA Performance Center 用户帐户。已经在 IdP 上定义的所有用户都将收到与您指定的用户帐户同等级别的产品权限。这些帐户也将传播到 CA Performance Center，其中它们作为新用户显示在用户列表中。在许多情况下，您必须编辑这些帐户，以确保这些用户仅可访问他们执行工作时所需的数据。

遵循这些步骤:

1. 以具有管理权限的用户身份登录 CA Performance Center。
2. 选择“管理”、“用户设置”，然后单击“用户”。

   “管理用户”页面将会打开。
3. 选择用户帐号来编辑。
4. 单击“编辑”。

   此时将打开“编辑用户”向导。
5. 选择“外部”作为身份验证类型。
6. 使用向导对用户帐户进行任何其他想要的更改。例如，前进到第三个向导对话框，为该用户选择不同的产品权限。
7. 单击“保存”。

   对用户帐户所做的更改已保存。

第 4 章： 单点登录使用 HTTPS

此部分包含以下主题：

安全套接字层 (SSL) 加密： HTTPS

默认情况下，单点登录使用 HTTP（超文本传输协议）在用户浏览器与 CA Performance Center 之间进行通信。TLS（传输层安全性）及其前身 SSL（安全套接字层）是广泛支持的加密协议，可保证 Internet 上数据传输的安全性。TLS 和 SSL 可与 HTTP 配合使用来形成 HTTPS (HTTP-Secure)。本指南使用 *SSL* 作为总括性术语表示“TLS 和 SSL”。

可以通过将单点登录配置为使用 HTTPS（而不是 HTTP）来增强监视系统中的安全性。

将 CA 单点登录配置为使用 HTTPS 是可选的。在您可以将单点登录网站配置为使用 HTTPS 之前，必须获得服务器证书。为您的组织创建和实施安全策略的团队可能需要通过这些步骤来帮助您。

如何为 CA 单点登录设置 HTTPS

要启用 SSL，需要执行几个步骤。首先，安装验证服务器身份的证书。其次，更改数据库，以便 CA Performance Center 正确地重定向到正确的端口和架构，以实现单点登录（反之亦然）。最后，更改 CA Performance Center 和单点登录的服务，以便反映新的端口和架构。

有两个端口对于这些步骤很重要：CA Performance Center 端口（默认为 8181）和单点登录端口（默认为 8381）。端口 8181 是 CA Performance Center 连接端口。如果用户需要进行身份验证，服务器会将他们重定向到端口 8381 的单点登录，在那里他们会看到登录页。一旦用户成功登录，服务器会将该用户重定向回端口 8181 的初始 URL。

因此，您无法在各个配置步骤中使用同一端口。否则，会在 CA Performance Center 和单点登录之间发生冲突。

要为 CA Performance Center 和单点登录启用 HTTPS，请完成下列步骤：

1. 获取服务器证书并将它安装在 Web 服务器 keystore 中 (p. 50)。
2. 使用单点登录配置工具更新必要属性 (p. 55)。
3. 在 CA Performance Center 控制台上设置 HTTPS (p. 56)。
4. 针对单点登录设置 HTTPS (p. 58)。
5. 停止并重新启动服务。

设置 SSL 证书

在可以配置单点登录网站以使用 HTTPS 之前，您必须获得和安装私钥以及关联的公共证书。SSL 可以与自签名证书或者信任的证书颁发机构已经签名的证书一起使用。这些步骤通常是组织和其安全团队的策略所特有的。但是，这些步骤提供了一些为您提供指导的信息。

选择适合您的情况的适当步骤：

- 生成并且导入新的证书 (p. 50)。
- 导入现有的证书 (p. 53)。

注意：有关用于这些步骤的 keytool 命令的更多信息，请参阅 Oracle 网站上的 Java 文档。

生成并且导入证书

如果还没有 SSL 证书，您可以使用 keytool 命令生成一个。此过程解释如何生成自签名证书并且将其安装在 keystore 中。

遵循这些步骤:

1. 运行以下命令：

   ```
   cd installDirectory/PerformanceCenter/jetty/etc
   ```

2. 使用以下命令重命名现有 jetty keystore 文件以创建其备份：

   ```
   mv installDirectory/PerformanceCenter/jetty/
   etc/keystore installDirectory/PerformanceCenter/
   jetty/etc/keystore.bak
   ```

   重要说明！必须删除旧的 keystore。否则会在后续步骤中显示错误消息：“Keystore 被篡改，或者密码不正确”。

3. 使用以下命令生成私钥和自签名的公共证书：

   ```
   keytool -genkeypair -keystore keystore_file.ks -storepass storepasswd
   -keyalg RSA -keysize 2048 -keypass keypasswd -alias alias_name
   ```

   storepasswd

   为 keystore 指定密码。

   keypasswd

   指定密钥库中的私钥密码。

   重要说明！记住这些密码 -- 它们无法恢复。

4. 使用下列命令从密钥库中导出自签名证书：

   ```
   keytool -exportcert -keystore keystore_file.ks -storepass storepasswd -alias
   alias_name -file filename.cer
   ```

   别名

   指定可用于引用为包含密钥而创建的密钥库条目的别名。

   filename.cer

   确定导出证书的目的文件。我们建议使用不将文件放到当前目录的完整路径名。

   示例：/tmp/capcCert.cer。

   注意：我们建议先备份 cacerts 文件，再继续操作。

5. 使用下列命令将自签名证书导入 Java 信任的证书密钥库：

   ```
   keytool -importcert -keystore installDirectory/jre/lib/security/cacerts
   -storepass cacertspasswd -alias capcSelfSigned -file filename.cer
   ```

   注意：cacerts keystore 的默认密码是“changeit”。

   cacertspasswd

   为 cacerts keystore 指定密码。

   默认： changeit

   filename.cer

   在前一个步骤中导出证书的目的文件。

6. 备份 cacerts 文件。

7. （可选）为提高安全性，使用以下命令更改 java 信任的证书 keystore 的密码：

   ```
   keytool -storepasswd -keystore installDirectory/jre/lib/security/cacerts
   ```

   系统会提示您提供现有密码和新密码。

8. 确认您导入的 keystore 可用。使用以下命令：

   ```
   keytool -list -keystore installDirectory/jre/lib/security/cacerts
   ```

   重要说明！要启用 Web 服务，自签名证书必须位于 cacerts keystore 中。否则，您会在日志中看到报告 PKIX 未找到证书的错误。

9. 使用这些命令重新启动各个 CA Performance Center 服务：

   ```
   /sbin/service caperfcenter_sso restart
   ```

   ```
   /sbin/service caperfcenter_devicemanager restart
   ```

   ```
   /sbin/service caperfcenter_console restart
   ```

   系统将生成您的自签名 SSL 证书并将其安装在 keystore 中。

后续步骤:

- （可选）将自签名证书转化成证书颁发机构 SSL 证书 (p. 52)
- 配置端口和网站以支持 HTTPS (p. 55)

将自签名证书转化成证书颁发机构 SSL 证书

在用户打开 CA Performance Center 时，自签名证书提示浏览器警告。要继续操作，用户可以手动忽略这项警告。不过，信任的证书颁发机构签名的证书不会出现浏览器警告。下列过程说明了如何将自签名证书转换成信任的证书颁发机构签名的证书。

遵循这些步骤:

1. 运行以下命令：

   ```
   cd installDirectory/PerformanceCenter/jetty/etc
   ```

2. 使用以下命令导出证书签名请求：

   ```
   keytool -certreq -keystore keystore_file.ks -storepass storepasswd -alias alias_name -keypass keypasswd -file requestFileName.csr
   ```

   ***requestFileName*.csr**

   确定导出的签名请求的路径和文件名。

3. 将所得文件 (*requestFileName*.csr) 与请求的任何其他信息一道发送到合格的签署机构。

   证书颁发机构将已签名的证书 (*signedCert*.cer) 发送给您。他们还可能提供根证书颁发机构证书 (*rootCA*.cer) 来对已签名的证书进行身份验证。

4. （*可选*）使用以下命令确定根证书颁发机构证书是否是 java 信任的默认机构的一部分：

   ```
   keytool -list -v -keystore installDirectory/jre/lib/security/cacerts -storepass cacertspasswd
   ```

5. （*可选*）搜索签署证书的证书颁发机构的输出。如果证书颁发机构未被列出，请使用以下命令将它添加到信任的颁发机构的列表中：

   ```
   keytool -importcert -keystore installDirectory/jre/lib/security/cacerts
   -storepass cacertspasswd -alias myRootCa -file rootCA.cer
   ```

6. 使用以下命令导入已签名的证书：

   ```
   keytool -importcert -trustcacerts -keystore keystore -storepass storepasswd
   -alias alias_name -keypass keypasswd -file signedCert.cer
   ```

7. 使用以下命令验证 jetty keystore 的内容：

   ```
   keytool -list -keystore
   installDirectory/PerformanceCenter/jetty/etc/keystore
   ```

   您导入的单个证书将显示在列表中。

8. 使用这些命令重新启动各个 CA Performance Center 服务：

   ```
   /sbin/service caperfcenter_sso restart

   /sbin/service caperfcenter_devicemanager restart

   /sbin/service caperfcenter_console restart
   ```

   证书颁发机构 SSL 证书将替换您的 keystore 中的自签名证书。

下一步：配置端口和网站以支持 HTTPS (p. 55)。

导入密钥和现有证书

您可以使用不同来源的私钥和公共证书（自签名证书或者证书颁发机构的证书）。例如，您的安全团队可以提供为您的组织定制的 SSL 证书。要使用此 SSL 证书，请导入私钥和已签名的证书。

遵循这些步骤:

1. 运行以下命令：

   ```
   cd /opt/CA/PerformanceCenter/jetty-version/etc
   ```

2. 使用以下命令删除旧的 keystore：

   ```
   rm keystore
   ```

3. 使用以下命令从私钥和证书创建 PKCS#12 密钥库：

   ```
   openssl pkcs12 -export -in certificate.pem -inkey privatekey.pem -name
   MyAlias
   -out keystore.pkcs12
   ```

   certificate.pem

   指定提供给您的证书。

   privatekey.pem

   指定提供给您的私钥。

   注意：此命令仅适用于 Linux。

4. 使用以下命令将密钥和证书导入 CA Performance Center 密钥库：

   ```
   keytool -importkeystore -destkeystore keystore_file -deststorepass
   storepasswd
   -srckeystore keystore.pkcs12 -srcstoretype pkcs12 -srcalias src_alias_name
   -destalias dest_alias_name -destkeypass keypasswd
   ```

5. 使用这些命令重新启动各个 CA Performance Center 服务：

   ```
   /sbin/service caperfcenter_sso restart

   /sbin/service caperfcenter_devicemanager restart

   /sbin/service caperfcenter_console restart
   ```

   系统将您现有的 SSL 证书导入到 keystore。

下一步：配置端口和网站以支持 HTTPS (p. 55)。

注意：如果证书不包括终止密钥存储中证书的链，则将证书导入 Java cacerts 密钥存储。运行以下命令以确定证书是否包括链：

```
keytool -printcert -file filename
```

文件名

指定证书的名称。

有关将证书导入 Java cacerts 密钥存储说明的信息，请参阅“生成和导入证书 (p. 50)”。

为 SSL 配置端口和网站

默认情况下，单点登录使用端口 8381。要设置 HTTPS，请使用单点登录配置工具更新默认网站方案和端口以与加密设置相匹配。

在安装数据源的每个服务器上执行此过程中的任务。

遵循这些步骤:

1. 在以下目录中运行“./SsoConfig”命令，以启动单点登录配置工具：

   ```
   [安装目录]/CA/PerformanceCenter
   ```

   系统会提示您选择一个选项。

2. 当您正在更改设置时，请在需要时使用以下命令：
   - q（退出）
   - b（返回上一级菜单）
   - u（更新）
   - r（重置）
3. 输入 1 以选择 CA Performance Center。
4. 输入 4 以配置单点登录。

   系统将提示您指定优先级。
5. 输入以下选项之一：

   1. 远程值

   指的是只有管理员可以更改的设置。此类设置将传播到注册到此 CA Performance Center 实例的所有其他 CA 产品。仅当相应的“本地覆盖”值不存在时，才能使用“远程值”设置。

   2. 本地覆盖

   指的是可以针对所有产品更改的设置。如果“本地覆盖”值存在，其优先级将高于“远程值”和默认设置。

   系统将提示您选择要配置的属性。
6. 为“方案”属性输入 12。
7. 输入 u 以更新值。
8. 为值提供“https”。

9. 为“端口”属性输入 13。
10. 将该值更新为“8382”。
11. 输入“b”两次以返回到“SSO 配置”/“CA Performance Center”菜单。
12. 输入“3”以配置性能中心。

    系统将提示您指定优先级。
13. 为“远程值”输入“1”或为“本地覆盖”输入“2”。
14. 输入“6”以选择网站方案。
15. 将该值更新为“https”。
16. 输入“8”以选择网站端口。
17. 将该值更新为“8182”。
18. 输入 q 以退出。

现在，您必须将 CA Performance Center 文件配置为使用 HTTPS。

配置 CA Performance Center 以使用 HTTPS

您必须编辑某些配置文件以反映新的网站和端口设置。编辑配置文件，将 HTTP 连接器替换为 HTTPS 连接器。您还必须重新启动 CA Performance Center 服务，才能使更改生效。

遵循这些步骤:

1. 转到以下目录：

   ```
   cd/[InstallationDirectory]/CA/PerformanceCenter/PC
   ```
2. 打开 start.ini 文件进行编辑。
3. 找到以下行并删除“#”，以便该行处于活动状态：

   ```
   #/opt/CA/PerformanceCenter/PC/etc/jetty-ssl.xml
   ```

   其中，“/opt/CA”是默认安装目录。
4. 保存 start.ini。
5. 转到以下目录：

   ```
   cd/[InstallationDirectory]/CA/PerformanceCenter/PC/etc
   ```

6. 使用以下内容在该目录中创建名为“jetty-ssl.xml”的文件：

```
<?xml version="1.0"?>
<!DOCTYPE Configure PUBLIC "-//Jetty//Configure//EN"
"http://www.eclipse.org/jetty/configure.dtd">
<Configure id="Server" class="org.eclipse.jetty.server.Server">
  <Call name="addConnector">
    <Arg>
      <New class="org.eclipse.jetty.server.ssl.SslSelectChannelConnector">
         <Set name="Port">8182</Set>
         <Set name="maxIdleTime">30000</Set>
        <Set name="Keystore"><Property name="jetty.home" default="."
/>/etc/keystore</Set>
        <Set name="Password">***PASSWORD***</Set>
         <Set name="KeyPassword">***PASSWORD***</Set>
        <Set name="truststore"><Property name="jetty.home" default="."
/>/etc/keystore</Set>
        <Set name="trustPassword">***PASSWORD***</Set>
        <Set name="allowRenegotiate">true</Set>
      </New>
    </Arg>
  </Call>
</Configure>
```

7. 将“***PASSWORD***”值的所有实例替换成您系统中正在使用的密码。

8. 保存文件。

9. 打开 jetty.xml 文件进行编辑。

10. 为默认 HTTP 连接器删除以下行：

```
<Call name="addConnector">
  <Arg>
      <New class="org.eclipse.jetty.server.nio.SelectChannelConnector">
          <Set name="host"><Property name="jetty.host" /></Set>
            <!-- Changed: Used to be Property -->
           <Set name="port"><SystemProperty name="jetty.port"
default="8181"/></Set>
           <Set name="maxIdleTime">300000</Set>
           <Set name="Acceptors">2</Set>
           <Set name="statsOn">false</Set>
           <Set name="confidentialPort">8443</Set>
           <Set name="lowResourcesConnections">20000</Set>
           <Set name="lowResourcesMaxIdleTime">5000</Set>
      </New>
  </Arg>
 </Call>
```

11. 保存 jetty.xml。

12. 转到以下目录：

```
cd/[InstallationDirectory]/CA/PerformanceCenter/PC/conf
```

13. 编辑文件 wrapper.conf。在以下行中，将“8181”替换为“8182”，以便与 jetty-ssl.xml 中所定义的端口相匹配（如前所述）：

    ```
    wrapper.java.additional.2=-Djetty.port=8181
    ```

14. 保存 wrapper.conf。

15. 转到以下目录：

    ```
    cd /[InstallationDirectory]/CA/PerformanceCenter/sso/webapps/
    sso/configuration
    ```

16. 编辑文件“CAPerformanceCenter.xml”。

17. 使用适合于 SSL 的设置替换 <Scheme> 和 <Port> 值：

    ```
    <?xml version="1.0" encoding="utf-8" ?>
    <Configuration>
        <SingleSignOnEnabled>True</SingleSignOnEnabled>
        <SingleSignOnProductCode>pc</SingleSignOnProductCode>
        <SignInPageProductDefaultUrl>
            <Scheme>https</Scheme>
            <Port>8182</Port>
            <PathAndQuery>/pc/desktop/page</PathAndQuery>
        </SignInPageProductDefaultUrl>
        <SingleSignOnWebServiceUrl>
            <Scheme>https</Scheme>
            <Port>8182</Port>
            <PathAndQuery>/pc/center/webservice/sso</PathAndQuery>
        </SingleSignOnWebServiceUrl>
    </Configuration>
    ```

更新单点登录配置并重新启动服务

编辑某些启动文件以在单点登录中支持 SSL 加密。您还必须重新启动所有 CA Performance Center 和单点登录服务才能更新设置。

遵循这些步骤:

1. 转到以下目录：

   ```
   cd/[InstallationDirectory]/CA/PerformanceCenter/sso
   ```

2. 打开 start.ini 文件进行编辑。

3. 找到以下行并删除“#”，以便该行处于活动状态：

   ```
   #/opt/CA/PerformanceCenter/sso/etc/jetty-ssl.xml
   ```

   其中，“/opt/CA”是默认安装目录。

4. 保存 start.ini。

5. 转到以下目录：

   ```
   cd/[InstallationDirectory]/CA/PerformanceCenter/sso/etc
   ```

6. 使用以下内容在该目录中创建名为 jetty-ssl.xml 的文件：

```
<?xml version="1.0"?>
<!DOCTYPE Configure PUBLIC "-//Jetty//Configure//EN"
"http://www.eclipse.org/jetty/configure.dtd">
<Configure id="Server" class="org.eclipse.jetty.server.Server">
  <Call name="addConnector">
    <Arg>
      <New class="org.eclipse.jetty.server.ssl.SslSelectChannelConnector">
         <Set name="Port">8382</Set>
         <Set name="maxIdleTime">30000</Set>
        <Set name="Keystore"><Property name="jetty.home" default="."
/>/etc/keystore</Set>
         <Set name="Password">***PASSWORD***</Set>
         <Set name="KeyPassword">***PASSWORD***</Set>
       <Set name="truststore"><Property name="jetty.home" default="."
/>/etc/keystore</Set>
         <Set name="trustPassword">***PASSWORD***</Set>
         <Set name="allowRenegotiate">true</Set>
      </New>
    </Arg>
  </Call>
</Configure>
```

7. 将“***PASSWORD***”值的所有实例替换成您系统中正在使用的密码。

8. 保存 jetty-ssl.xml。

9. 打开文件 jetty.xml。

10. 为默认 HTTP 连接器删除以下行：

```
<Call name="addConnector">
  <Arg>
      <New class="org.eclipse.jetty.server.nio.SelectChannelConnector">
          <Set name="host"><Property name="jetty.host" /></Set>
            <!-- Changed: Used to be Property -->
           <Set name="port"><SystemProperty name="jetty.port"
default="8181"/></Set>
           <Set name="maxIdleTime">300000</Set>
           <Set name="Acceptors">2</Set>
           <Set name="statsOn">false</Set>
           <Set name="confidentialPort">8443</Set>
           <Set name="lowResourcesConnections">20000</Set>
           <Set name="lowResourcesMaxIdleTime">5000</Set>
      </New>
  </Arg>
 </Call>
```

11. 保存 jetty.xml。

12. 转到以下目录：

```
[安装目录]/CA/PerformanceCenter/sso/conf
```

13. 编辑文件 wrapper.conf。在以下行中，将“8381”替换为“8382”，以便与 jetty-ssl.xml 中所定义的端口相匹配（如前所述）：

    ```
    wrapper.java.additional.2=-Djetty.port=8381
    ```

14. 保存 wrapper.conf。

15. 通过输入以下命令停止控制台、设备管理器和 SSO 服务：

    ```
    service caperfcenter_console stop

    service caperfcenter_devicemanager stop

    service caperfcenter_sso stop
    ```

16. 通过输入以下命令重新启动服务

    ```
    service caperfcenter_sso start

    service caperfcenter_devicemanager start

    service caperfcenter_console start
    ```

第 5 章： 故障排除

此部分包含以下主题：

浏览器显示错误

症状：

在登录页面上输入密码时，Web 浏览器重定向到一个错误页面。我是否键入了错误的密码？

解决方案：

该症状不表示您输入了错误的 SAML 凭据。相反，浏览器错误（如 401 或 500）表示单点登录将浏览器重定向至登录 URL，但是身份提供商 (IdP) 服务器已关闭。

执行下列步骤：

- 验证 IdP 服务器是否正在运行。
- 测试 CA Performance Center 服务器和 IdP 服务器之间的网络连接。

Logs

通过每天或每周检查日志文件，可在问题影响正常运行之前解决问题。所有日志都存储在与相关服务（或后台进程）对应的子文件夹中。在以下路径中查找日志文件：

```
CA/PerformanceCenter/<servicename>/logs
```

将 *servicename* 参数替换成下列服务名称之一：

DM

设备管理器。

- DMService.log - 设备管理器的输出，主要与同步有关。
- wrapper.log -caperfcenter_devicemanager 过程日志记录。

EM

事件管理器。

- EMService.log - 事件管理器的输出；包括事件和报警的详细信息。
- wrapper.log - caperfcenter_eventmanager 过程日志记录。

PC

主控制台程序。

- PCService.log - CA Performance Center 相关的日志记录；包括用户界面和视图组件。
- wrapper.log - caperfcenter_console 过程日志记录。

SSO

Single Sign-On 身份验证软件。

- SSOService.log - Single Sign-On 日志记录，其中包括已配置 HTTPS 的 HTTPS（安全套接字层）信息。
- wrapper.log - caperfcenter_sso 过程日志记录。

有关 Single Sign-On 配置工具存在的问题，请检查位于以下位置的应用程序日志：

```
/opt/CA/PerformanceCenter/sso/logs/application.log
```

日志文件名包括相关日期和时间。

每天会自动生成新日志文件。较旧的日志文件将在 14 天后自动删除，以免占用过多磁盘空间。

访问最新的日志文件，以查找与数据库或数据源同步关联的错误。可以首先从“显示板”选项卡打开“事件”显示板并按“状态”排序。如果要查看相关的日志文件，请注意事件类型以及失败日期和时间。在日志目录中，打开文件名中包含相应日期的日志文件。

检查审核日志

通过将有关用户登录活动的日常详细信息记录到文件中，单点登录支持安全审核。检查日志以验证用户活动。

遵循这些步骤:

1. 登录到安装了 CA 数据源产品的服务器。
2. 打开命令提示符，并使用 cd 转到以下目录：

   `[InstallationDirectory]/PerformanceCenter/sso/logs`

   注意：审核日志在 Windows 服务器上保存在以下位置：
   `[安装目录]\Portal\SSO\logs.`
3. 输入 dir 以查看该目录的内容。

   日志文件的文件名是 SingleSignOnAuditLogyyyy-mm-dd.log。
4. 输入要查看的审核文件的名称。

   该文件将在本地文本编辑器应用程序中打开。

词汇表

LDAP

LDAP（轻量级目录访问协议）是一种协议，用于指定在 IP 网络中搜索和编辑目录并存储目录信息的方式。此外，因为 LDAP 包括身份验证组件，所以常常用于确保网络访问安全。通常将 LDAP 目录组成单元的逻辑组。Microsoft Active Directory 是使用 LDAP 的目录应用程序的典型示例。

SAML

安全断言标记语言 (*SAML*) 是基于 XML 的安全协议。基本概念涉及关于请求对安全域的访问权限的对象（人或计算机）的安全断言的交换。断言包括对象是否可以访问特定资源，以及是否使用外部数据源（如策略存储）。

SSL

SSL（安全套接字层）是一种加密协议，许多 Web 浏览器支持该协议，从而在 Internet 上实现数据安全性。服务器交换 SSL 证书，其中包含用于对交换的数据进行加密的公钥和用于对相应数据进行解密的私钥。SSL 允许 Web 浏览器指定基于浏览器、客户端计算机和服务器功能来使用的加密级别。最高级别是 256 位加密，解密难度最高。

TLS

TLS（传输层安全性）及其前身 SSL（安全套接字层）是广泛支持的加密协议，可保证 Internet 上数据传输的安全性。SSL/TLS 可与 HTTP 配合使用来形成 HTTPS (HTTP-Secure)。

身份提供商 (IdP)

身份提供商 (IdP) 存储身份或安全信息，并在请求进行身份验证时提供这些信息。也称为“断言方”（SAML 身份验证所需要的三个组件角色之一）。

单点登录

*单点登录*是用于 CA Performance Center 和所有受支持数据源的身份验证方案。在用户经身份验证有权访问 CA Performance Center 之后，他们无需再次登录即可在控制台和注册的数据源中导航。

配置工具

*配置工具*是一个命令行应用程序，允许管理员调整单点登录网站和关联的 CA 数据源产品使用的设置。