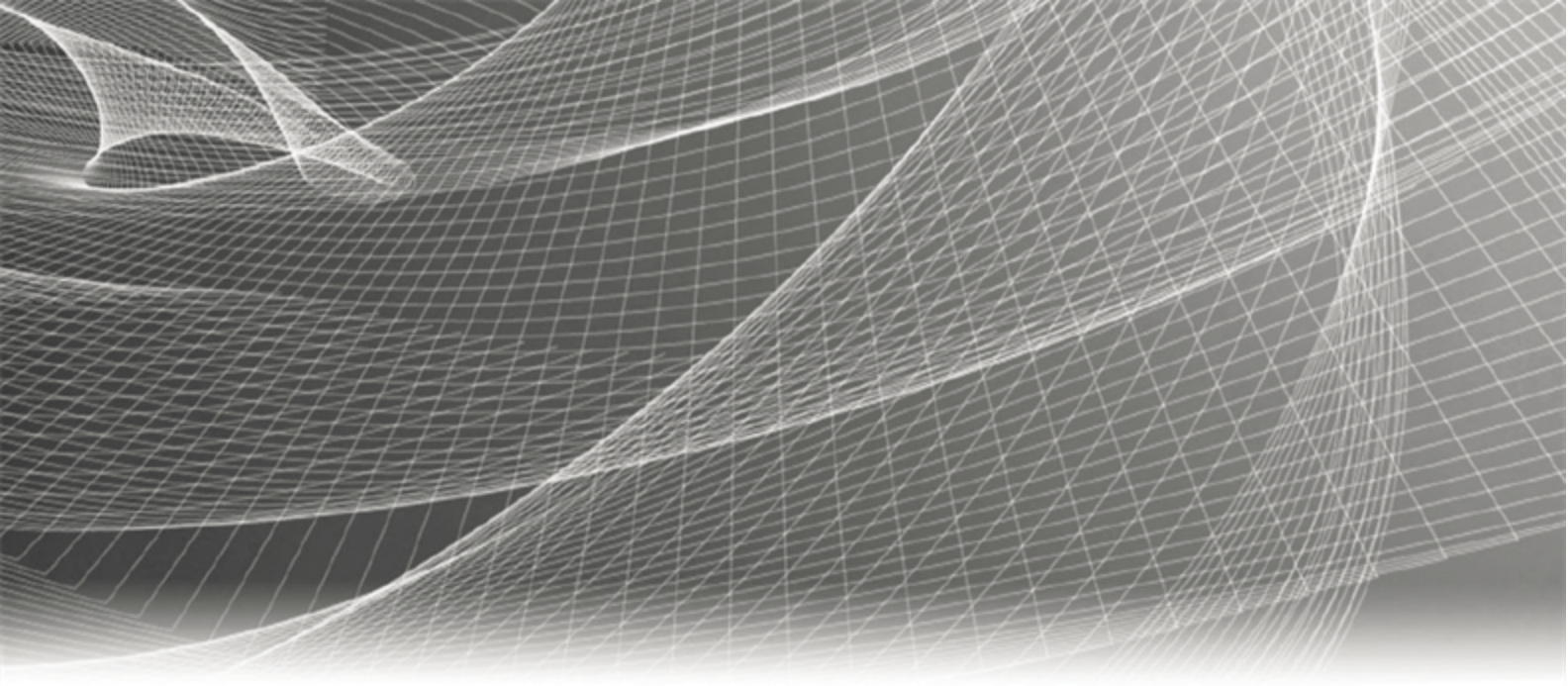

RSA SECURID® ACCESS

RSA SecurID® Authentication Agent 8.0 for PAM

适用于 AIX 的安装和配置指南

联系信息

RSA Link https://community.rsa.com 包含一个知识库，该库可提供常见问题解答并针对已知问题、产品文档、社区讨论和案例管理提供解决方案。

商标

Dell、RSA、RSA 徽标、EMC 和其他商标为 Dell Inc. 或其子公司的商标。其他商标可能是其各自所有者的商标。要查看 RSA 商标的列表，请访问 http://www.emc2.com.cn/zh-cn/legal/emc-corporation-trademarks.htm。

许可协议

本软件及关联的文档是 Dell Inc. 或其子公司的专有和机密内容，依据许可证提供，仅在遵守此类许可证条款的情况下才能使用和拷贝，并应在使用和拷贝时包括下面的版权声明。本软件和文档及其任何拷贝不可提供给其他任何人或以其他方式供其使用。

软件或文档的拥有权或所有权或任何知识产权不会随之转移。未经授权使用或复制本软件和文档可能会面临民事和/或刑事责任。

本软件随时可能更改，恕不另行通知，且不应将其理解为 Dell Inc. 所做的承诺。

第三方许可证

本产品可能包括 RSA 以外的厂商开发的软件。可通过 RSA Link，在产品文档页面上查看适用于本产品中第三方软件的许可协议的文本。使用本产品即表示本产品的用户同意完全受许可协议条款的约束。

加密技术备注

本产品可能包含加密技术。很多国家/地区禁止或限制使用、进口或出口加密技术，在使用、进口或出口本产品时，应遵守现有的使用、进口和出口法规。

分发

使用、复制或分发本出版物所描述的任何 Dell 软件都要有相应的软件许可证。

Dell Inc. 确信本出版物在发布之日内容准确无误。该信息如有更改，恕不另行通知。

本出版物的内容按"原样"提供。DELL INC. 对本出版物的内容不提供任何形式的陈述或担保，明确拒绝对有特定目的的适销性或适用性进行默示担保。

2017 年 12 月

目录

前言

受众

本指南适用于安装和升级 RSA SecurID® Authentication Agent for PAM（可插拔身份验证模块）并对其进行故障排除的网络和系统管理员。

支持和服务

可访问 RSA Link 上的社区和支持信息，网址为：https://community.rsa.com。RSA Link 包含一个知识库，其中回答常见问题，并提供针对已知问题、产品文档、社区讨论和案例管理的解决方案。

RSA Ready 合作伙伴计划

RSA Ready 合作伙伴计划网站 www.rsaready.com 提供有关经过认证可与 RSA 产品配合使用的第三方硬件和软件产品的信息。该网站中提供了《实施指南》，其中包含有关 RSA 产品如何与第三方产品配合使用的分步说明和其他信息。

第 1 章：安装 PAM Agent

RSA SecurID Authentication Agent 8.0 for PAM 概述

RSA SecurID Authentication Agent 8.0 for PAM(可插拔身份验证模块) 支持使用标准或 OpenSSH 连接工具的 UNIX 系统上的身份验证。PAM Agent 使用 RSA 自定义共享库，并支持使用 Cloud Authentication Service 和 RSA Authentication Manager 支持的身份验证方法访问 UNIX 服务器和工作站。

您可以选择 PAM Agent 是向 Cloud Authentication Service 还是Authentication Manager 进行身份验证。RSA SecurID Access Enterprise Edition 许可证和 Premium Edition 许可证包括 RSA SecurID Access 的这两个组件。Authentication Manager 不是使用 PAM Agent 所必需的。

8.0 版 PAM Agent 提供以下新优势：

- 支持 Cloud Authentication Service。Cloud Authentication Service 使用多因素身份验证方法，例如批准(针对移动设备优化的推送通知) 、Authenticate Tokencode、设备生物识别和 RSA SecurID 令牌，可帮助用户安全地访问软件即服务 (SaaS) 和内部部署 Web 应用程序。
- 能够使用 REST 协议而不是 UDP 协议访问 Authentication Manager。
- 继续支持较早版本的 PAM Agent 使用的 UDP 协议。
- Authentication Manager 提供有代理报告，可帮助您管理使用 REST 协议的已安装 PAM Agent。在 REST 模式中，PAM Agent 可以向 Authentication Manager 服务器发送附加信息，例如安装的每个 PAM Agent 的唯一软件 ID 号和有关代理使用的操作系统的信息。

在 REST 模式下使用 PAM Agent 比使用 UDP 协议具有更多优点：

- 使您的 Authentication Manager 部署能够轻松集成 Cloud Authentication Service。
- 您可以在 Authentication Manager 中添加和维护一个身份验证代理记录，并使用它来表示多个已安装的代理。
- 与使用 UDP 协议相比，您可以更容易地在同一硬件上运行多个身份验证代理。
- 对要求身份验证代理使用 IPv4 网络设置或 IPv4 协议的部署使用 TCP 协议。
- 在 REST 协议身份验证模式下，PAM Agent 8.0 版将符合 FIPS 标准的加密库模块 **fips-2.0.16** 与 OpenSSL 1.0.21 版结合使用。有关详细信息，请参阅 *OpenSSL FIPS 140-2 安全策略版本 2.0.16*，网址为：https://www.openssl.org/docs/fips/SecurityPolicy-2.0.16.pdf。
- 与不使用 REST 协议的身份验证代理相比，需要更少的身份验证代理更新即可实现新功能和增强功能。使用 REST 协议的身份验证代理更有可能利用 Authentication Manager 中的更改，从而减少多个代理上所需的更新数量。

身份验证模式

您可以采用三种身份验证模式之一安装 PAM Agent。所有模式都提供 RSA SecurID 身份验证。可以根据需要在安装后更改模式。有关说明，请参阅更改 PAM Agent 身份验证模式 在本页 29。

身份验证模式	描述
采用 UDP 协议的 RSA Authentication Manager	RSA SecurID 硬件和软件身份验证器生成 RSA SecurID 令牌代码。代理验证用户输入的数据是否与 Authentication Manager 中存储的数据匹配，并根据结果允许或拒绝访问。 默认情况下，PAM Agent 升级将代理配置为使用 UDP 协议。您可以轻松切换到使用 REST 协议的不同身份验证模式。
采用 REST 协议的 RSA Authentication Manager	支持 Authentication Manager 通过 REST 协议支持的所有类型的身份验证，例如 RSA SecurID 软件和硬件令牌以及通过与 Cloud Authentication Service

身份验证模式	描述
	组件集成获得的 Authenticate Tokencode。
采用 REST 协议的 Cloud Authentication Service	支持批准（针对移动设备优化的推送通知）、Authenticate Tokencode、设备生物识别和 RSA SecurID 令牌。不支持 FIDO 令牌、SMS 令牌码和语音令牌码。

RSA SecurID Authentication Agent 8.0 for PAM 支持 RSA Authentication Manager 受信任域。不支持 Authentication Manager 基于风险的身份验证 (RBA)。

PAM Agent 工作流

PAM Agent 安装在 UNIX 服务器上。它充当进行身份验证的用户与 RSA Authentication Manager 服务器或 Cloud Authentication Service 之间的中介。

PAM Agent 支持 Authentication Manager 安全功能。例如，如果 Authentication Manager 确定与特定令牌关联的用户需要新的 PIN，则代理会请求具有 Authentication Manager 中所定义特征的 PIN，并将信息发送给 Authentication Manager。如果 Authentication Manager 请求用户的令牌上显示的下一个令牌码，则 PAM Agent 会提示用户。如果没有将正确的下一个令牌码发送到 Authentication Manager，则身份验证将失败。

这些步骤描述了 PAM Agent 在全部三种身份验证模式下的身份验证流程：

1. 用户尝试在本地（使用 login）或远程（使用 rlogin、telnet、SSH 和 FTP 等工具）访问受 PAM Agent 保护的计算机。

   用户必须位于安装了 PAM Agent 的计算机本地。

2. UNIX 可插拔身份验证模块 (PAM) 基础架构能够截取所有登录请求，并使用 PAM 配置文件来访问 RSA PAM 模块：
   - 如果用户未配置为使用 RSA SecurID 身份验证，则 RSA PAM 模块允许请求成功。
   - 如果请求访问的用户受到 RSA SecurID 的质询，则 PAM Agent 继续执行步骤 3 的身份验证。
3. 根据 PAM Agent 的身份验证模式，代理会联系 Authentication Manager 或 Cloud Authentication Service。

   对于使用 UDP 连接或 REST 协议的 Authentication Manager，将执行以下步骤：

   a. 代理提示用户输入用户名，然后输入密码。
   b. 代理安全地将用户名和密码发送到 Authentication Manager：
      - 如果 Authentication Manager 批准请求，代理将向用户授予访问权限。
      - 如果 Authentication Manager 不批准请求，代理将拒绝访问。

   对于 Cloud Authentication Service，将执行以下步骤：

   a. 代理提示用户输入用户名，然后将信息发送到 Cloud Authentication Service。
   b. Cloud Authentication Service 为代理提供在 Cloud Authentication Service 访问策略的保证级别为用户配置的身份验证方法。
   c. 代理提示用户进行身份验证。
   d. 用户选择可用的身份验证方法，并进行身份验证：
      - 如果 Cloud Authentication Service 批准请求，代理将向用户授予访问权限。
      - 如果身份验证方法不成功，Cloud Authentication Service 将提示用户选择下一个身份验证方法。
      - 如果 Cloud Authentication Service 不批准请求，代理将拒绝访问。

软件要求

本部分介绍了 PAM Agent 支持的最低软件版本。

所需的操作系统

PAM Agent 需要下列操作系统之一：

- AIX 7.1 TL3 (SP5) Power 6：32 位和 64 位
- AIX 7.2 TL1 (SP2) Power 8：32 位和 64 位

PAM Agent 包含 64 位库，以支持 IBM AIX 64 位操作系统上的 64 位工具。

必须在 PAM Agent 计算机上安装相应的 32 位或 64 位版本的 **libuuid.so**（ UUID 库）。

RSA Authentication Manager 版本支持

RSA Authentication Manager 支持 RSA SecurID 身份验证 API 版本 1.1，它是最新版本的 REST API。

下表列出支持特定的功能所需的 RSA Authentication Manager 版本。

需要的 RSA Authentication Manager 版本	支持的功能
8.2 SP1 或更高版本	PAM Agent 需要 RSA Authentication Manager 8.2 SP1 或更高版本。
8.2 SP1 Patch 5 或更高版本	如果在 PAM Agent 上启用代理报告标志，则需要使用 RSA Authentication Manager 8.2 SP1 Patch 5 或更高版本，以避免 REST 模式下的身份验证失败。
8.3	RSA Authentication Manager 8.3 包括帮助您管理已安装的 REST 协议 PAM Agent 的代理报告。这些报告中包括 PAM Agent 可以发送到 Authentication Manager 的其他信息。

Cloud Authentication Service 版本支持

RSA Authentication Manager 支持 RSA SecurID 身份验证 API 版本 1.1，它是最新版本的 REST API。

证书要求

PAM Agent 对 REST 协议使用 TLS 1.2 证书。Cloud Authentication Service 和 RSA Authentication Manager 8.2 版或更高版本可以接受这些证书。不使用 TLS 1.2 证书的部署必须使用支持采用 UDP 协议的 Authentication Manager 的身份验证模式。

在 REST 协议身份验证模式下，PAM Agent 将符合 FIPS 标准的加密库模块 **fips-2.0.16** 与 OpenSSL 1.0.21 版结合使用。有关详细信息，请参阅 *OpenSSL FIPS 140-2 安全策略版本 2.0.16*，网址为：https://www.openssl.org/docs/fips/SecurityPolicy-2.0.16.pdf。

支持的工具

PAM Agent 支持以下工具：

- telnet
- login

- rlogin
- su
- ssh(ssh、sftp 和 scp)
- sudo

  从 https://www.sudo.ws 下载并安装受支持的 sudo 版本。

- ftp(限制为单个事务)
- dtlogin

OpenSSH 支持(可选)

PAM Agent 支持 OpenSSH 6.0 P1。如果您使用 OpenSSH，请确认您的平台使用的是 OpenSSH 的兼容版本。OpenSSH 不是必需的。

支持以下可选的 OpenSSH 工具：

- ssh
- sftp
- scp

在代理计算机上安装 OpenSSH。有关 OpenSSH，包括前提条件和编译源代码所需的其他软件，请参阅 https://www.openssh.com。

规划 PAM Agent 的安装

在安装 PAM Agent 之前，请执行以下操作：

- 在要安装 PAM Agent 的计算机上：
  1. 获取根权限。
  2. 为 PAM Agent 配置文件创建 **/var/ace** 目录(如果不存在该目录) ，并创建安装目录。
  3. 从 RSA Authentication Manager 或 Cloud Authentication Service 获取服务器信任的根 CA 证书。请执行下列操作：
     a. 验证该证书未过期。
     b. 以 PEM 格式存储证书。如果有多个 CA 证书，则需要将它们合并成 PEM 格式的单个文件。
     c. 将 ***filename*.pem** 拷贝到 **/var/ace/** 目录中。
     d. 使用相应的权限保护包含证书的 **/var/ace/** 目录。
- 要使用 RSA Authentication Manager 进行身份验证，请在内部数据库中为 PAM Agent 创建身份验证代理记录。有关详细信息，请联系您的 Authentication Manager 超级管理员或参阅 RSA Link 上的 Authentication Manager 帮助。
- 要使用 UDP 协议进行身份验证，您必须生成 Authentication Manager 配置文件 **sdconf.rec**，或从您的 Authentication Manager 超级管理员那里获取此文件。使用 REST 协议的身份验证不需要此文件。

  sdconf.rec 文件指定代理如何通过 IP 地址与 Authentication Manager 主实例和复制副本实例通信。请执行下列操作：

  - 确保最新版本的 **sdconf.rec** 文件位于代理计算机上的可访问目录中，例如默认的 **/var/ace** 目录。
  - 您必须对存储 **sdconf.rec** 文件的目录拥有写入权限。

- 在对 Cloud Authentication Service 使用 REST 协议的身份验证模式中，PAM Agent 依赖于 Cloud Authentication Service 进行负载均衡和故障切换。
- 在对 RSA Authentication Manager 使用 REST 协议的身份验证模式中，PAM Agent 不支持负载平衡。PAM Agent 支持故障切换到最多 15 个 Authentication Manager 复制副本实例。
- 收集在安装 PAM Agent 时将要提供的信息。

采用 UDP 协议的 Authentication Manager。您可以保留默认值或指定新目录。

描述	规划
sdconf.rec 所在的目录。默认值为 **/var/ace/**。	
PAM Agent 目录的根路径。默认值为 **/opt**。	

采用 REST 协议的 Authentication Manager。向 Authentication Manager 超级管理员询问以下信息：

描述	规划
身份验证代理和 Authentication Manager 主实例之间的通信的 REST 服务器 URL。例如，https://*HOSTNAME*:*PORT_NO*/mfa/v1_1/authn	
可用于故障切换的 Authentication Manager 复制副本实例数。	
每个复制副本实例的 REST 服务器 URL。例如，https://*HOSTNAME*:*PORT_NO*/mfa/v1_1/authn。	
用于安全地将用户身份验证请求传递给 Authentication Manager 的访问密钥（客户端密钥）。该值在 Authentication Manager 主实例的安全控制台中生成。	
在身份验证代理上，输入服务器可信证书的目录和文件名。默认值是 **/var/ace/cert.pem**。	
在 Authentication Manager 中为 PAM Agent 创建的身份验证代理名称（客户端 ID）。	
PAM Agent 目录的根路径。默认值为 **/opt**。	

采用 REST 协议的 Cloud Authentication Service。向 Cloud Authentication Service 超级管理员询问以下信息：

描述	规划
代理与 Cloud Authentication Service 之间的通信的 REST 服务器 URL。例如，https://*HOSTNAME*:*PORT_NO*/mfa/v1_1/authn	
在 Cloud Administration Console 中创建的身份验证 API 密钥（客户端密钥），用于安全地将用户身份验证请求传递给 Cloud Authentication Service。	
在身份验证代理上，服务器受信任证书的目录和文件名。默认值是 **/var/ace/cert.pem**。	
Cloud Authentication Service 的租户 ID。PAM Agent 可以在身份验证请求中提供租户 ID，但代理不会验证该数据。Cloud Authentication Service 目前不支持此参数。	
Cloud Authentication Service 的访问策略名称。此策略在 Cloud Administration Console 中定义。	
要显示在移动通知中的 CLIENT_ID 身份验证代理名称。您可以输入任何	

描述	规划
值。例如，PAM_Agent。	
PAM Agent 目录的根路径。默认值为 **/opt**。	

安装 RSA SecurID Authentication Agent 8.0 for PAM

完成以下任务以安装 PAM Agent：

1. 启用 PAM 身份验证 向下
2. 指定 UDP 模式的代理 IP 地址 向下
3. 配置 OpenSSH 下一页
4. 安装 PAM Agent 下一页
5. 对于 UDP 模式，执行测试身份验证。有关详细信息，请参阅 UDP 模式的身份验证应用工具 在本页 35。

   对于 REST 协议模式，通过任何浏览器或 http 客户端访问 REST 服务器 URL 来测试连接。例如，输入 https://*HOSTNAME*:*PORT_NO*/mfa/v1_1/authn。由于您目前没有进行身份验证，因此您的浏览器或 http 客户端应显示"禁止"或"未授权"HTTP 响应。

启用 PAM 身份验证

要在 AIX 应用程序中提供 PAM 身份验证，您必须首先启用 PAM 身份验证。

过程

1. 在将安装 PAM Agent 的计算机上，切换到 **/etc/security** 目录，并打开 **login.cfg** 文件。
2. 注释以下行：

   ```
   auth_type = STD_AUTH
   ```

3. 启用 PAM 身份验证。键入：

   ```
   auth_type = PAM_AUTH
   ```

4. 保存文件。

指定 UDP 模式的代理 IP 地址

对于 UDP 模式，您必须在 **sdconf.rec** 文件使用的同一目录中创建 **sdopts.rec** 文件。此过程不适用于 REST 模式。

文件	描述
sdopts.rec	列出安装代理的计算机的 IP 地址。代理将使用 **sdopts.rec** 文件中的 IP 地址 与 RSA Authentication Manager 通信。
sdconf.rec	指定 Authentication Manager 使用的 IP 地址。

过程

1. 在代理计算机上，使用文本编辑器在保存 **sdconf.rec** 文件的路径中创建 **sdopts.rec** 文件。
2. 在文件中，键入以下内容：

   ```
   CLIENT_IP=x.x.x.x
   ```

其中 *x.x.x.x* 是代理主机的 IP 地址。

注意：仅使用大写字母，并且不要包含空格。

3. 保存文件。

配置 OpenSSH

如果您正在使用基于安全外壳 (SSH) 协议的与安全性相关的网络应用工具套件 OpenSSH，则必须将此软件配置为与 PAM Agent 协同工作，并向用户显示通行码身份验证消息。

准备工作

在代理计算机上安装 OpenSSH。有关 OpenSSH，包括前提条件和编译源代码所需的其他软件，请参阅 https://www.openssh.com。

过程

1. 在代理计算机上，打开 **sshd_config** 文件。
2. 设置以下参数，并保存所做更改：

参数	设置
UsePAM	yes
PasswordAuthentication	no
UsePrivilegeSeparation	no
ChallengeResponseAuthentication	yes

将 PasswordAuthentication 参数设置为 no 将禁用 OpenSSH 密码提示。改为使用 PAM Agent。结果是，系统仅提示用户进行 SecurID 身份验证。

3. 重新启动 sshd。键入：

```
service sshd restart
```

安装 PAM Agent

您可以手动将 PAM Agent 安装在个别计算机上，也可以选择静默式安装以自动执行部署 PAM Agent 多个副本的过程。

在一台计算机上安装 PAM Agent

执行此任务可安装一个 PAM Agent。要在多个计算机上安装 PAM Agent，请参阅使用静默式安装批量安装 PAM Agent 下一页。

过程

1. 在代理计算机上，切换到 PAM Agent 安装目录。
2. 通过键入以下命令解包文件：

```
tar -xvf filename.tar
```

3. 通过键入以下命令运行安装脚本：

```
/filename/install_pam.sh
```

4. 按照提示操作。按 Enter 键以接受默认值，或输入适当的值。

   对于 RSA Authentication Manager UDP 模式，执行以下操作：

   - 接受 RSA 软件许可证。
   - 输入 0 以选择使用 UDP 协议身份验证模式的 RSA Authentication Manager。
   - 输入 **sdconf.rec** 所在的目录。
   - 输入 PAM Agent 安装目录。

   对于 RSA Authentication Manager REST 模式，执行以下操作：

   - 接受 RSA 软件许可证。
   - 输入 1 以选择使用 REST 协议身份验证模式的 RSA Authentication Manager。
   - 输入身份验证代理和主实例之间的通信的 REST 服务器 URL。
   - 如果存在用于故障转移的 Authentication Manager 复制副本实例，请输入 y。
   - 指定复制副本实例的数量。
   - 输入每个复制副本实例的 REST 服务器 URL。
   - 输入用于安全地将身份验证请求传递给 Authentication Manager 的客户端密钥(访问密钥) 。
   - 在身份验证代理上，输入服务器可信证书的目录和文件名。
   - 输入客户端 ID，即 Authentication Manager 中的身份验证代理名称。
   - 输入 PAM Agent 安装目录。

   对于 Cloud Authentication Service REST 模式，执行以下操作：

   - 接受 RSA 软件许可证。
   - 输入 2 以选择使用 REST 协议身份验证模式的 Cloud Authentication Service。
   - 输入用于在身份验证代理和 Cloud Authentication Service 之间通信的 REST 服务器 URL。
   - 输入用于安全地将身份验证请求传递给 Cloud Authentication Service 的客户端密钥(身份验证 API 密钥) 。
   - 在身份验证代理上，输入服务器可信证书的目录和文件名。
   - 输入 Cloud Authentication Service 的租户 ID。
   - 输入 Cloud Authentication Service 的访问策略名称。
   - 输入要显示在移动通知中的 CLIENT_ID 身份验证代理名称。
   - 输入 PAM Agent 安装目录。

5. 仅限 UDP 模式，确认 **/etc/sd_pam.conf** 文件中的 VAR_ACE 指向 **sdconf.rec** 文件的正确位置。这是配置文件的路径。整个路径必须具有 -rw------- 根权限。

完成之后

- 您可以通过检查 PAM Agent 安装目录中的 **installer.log** 文件来验证安装。
- 对于 UDP 模式，执行测试身份验证。有关详细信息，请参阅 UDP 模式的身份验证应用工具 在本页 35。
- 对于 REST 协议模式，通过任何浏览器或 http 客户端访问 REST 服务器 URL 来测试连接。例如，输入 https://*HOSTNAME*:*PORT_NO*/mfa/v1_1/authn。由于您目前没有进行身份验证，因此您的浏览器或 http 客户端应显示"禁止"或"未授权"HTTP 响应。

使用静默式安装批量安装 PAM Agent

执行此任务可使用相同的配置信息部署大量 PAM Agent。例如，如果您需要安装大量与相同 RSA Authentication

Manager 服务器或相同 Cloud Authentication Service 进行通信的代理，请执行此任务。

准备工作

手动安装 PAM Agent，并记录提示。有关说明，请参阅在一台计算机上安装 PAM Agent 在本页 16。

过程

1. 创建一个基于文本的配置文件，可在其中指定 PAM Agent 安装脚本的配置选项。您可为配置文件选择任何名称，例如 **installoptions.conf**。
2. 打开文件，并按照提示在手动安装 PAM Agent 期间出现的相同顺序，在单独的行中列出要选择的每个配置选项。

   以下示例描述了 UDP 配置中指定的每个选项的相应提示：

示例值	选项
y	继续静默式安装？(y) 始终最先包含此提示。
Accept	接受许可条款和条件？（接受）
/var/ace	目录包含 sdconf.rec？（目录路径）
/opt	PAM Agent 目录的安装路径？（目录路径）
y	升级/覆盖现有安装？(y/n)
	（可选）如果前一个选项为"n"，是否使用备用根路径？（目录路径）

   在这种情况下，基于文本的配置文件将包含：

```
y
Accept
/var/ace
/opt
y
```

   再例如，对于 Authentication Manager REST 模式，配置文件可能包含类似如下的数据：

```
y
Accept
1
https://am821.example.com:5555/mfa_v1_1/authn
0i78x21rih887gb48126ufxh4g63orh3a3rt28k5416a2b3jxh05h86i7gntjfh3
/var/ace/cert.pem
sp7-dp33.network.com
/opt
y
```

   注意：安装提示的数量和顺序取决于 PAM Agent 模式和您正在安装的平台。

3. 切换到 PAM Agent 安装目录。
4. 通过键入以下命令解包文件：

```
tar -xvf filename.tar
```

5. 通过键入以下命令运行安装脚本：

   /filename/*install_pam.sh -s < *installoptions.conf

   其中 ***installoptions.conf*** 是您在步骤 1 中创建的配置文件。如果配置文件不在当前目录中，请指定 ***installoptions.conf*** 文件的完整路径。

升级到 RSA SecurID Authentication Agent 8.0 for PAM

您可以从版本 7.1 Patch 2 (7.1.0.2) 升级到 RSA SecurID Authentication Agent 8.0 for PAM。默认情况下，已升级的代理使用 RSA Authentication Manager 和 UDP 协议进行身份验证。您可以更改身份验证模式，以充分利用 Cloud Authentication Service 或 Authentication Manager 和 REST 协议。有关说明，请参阅更改 PAM Agent 身份验证模式 在本页 29。

准备工作

- 您必须在代理主机上拥有 root 权限，并对存储 **sdconf.rec** 文件的目录拥有写入权限。此文件通常存储在默认 **/var/ace** 目录中。
- 在覆盖前备份配置文件以保存配置设置。有关详细信息，请参阅关键配置文件 在本页 45。
- 将 RSA SecurID 保护的工具配置为使用随操作系统提供的标准 PAM 模块，而不是 RSA PAM 模块。在继续升级之前，必须先关闭使用 RSA PAM 模块的任何活动会话。

过程

1. 在代理计算机上，切换到 PAM Agent 安装目录。
2. 通过键入以下命令解包文件：

   `tar -xvf` ***filename.tar***

3. 通过键入以下命令运行安装脚本：

   /<filename>/install_pam.sh

4. 覆盖现有安装文件。在安装程序提示您覆盖当前安装时，键入 **y**。
5. 获取代理版本号，以确定升级是否成功：
   a. 切换到 ***PAM AgentInstall Directory*\lib*bit version*** 目录。
   b. 键入：

      strings pam_securid.so | grep "Agent"

      此命令将返回所安装代理的版本号。

6. 如果代理版本号未更改且升级不成功，请运行以下命令，然后重复升级步骤：

   `/usr/sbin/slibclean`

配置工具

您必须配置支持的工具来提示用户使用 Cloud Authentication Service 和 RSA Authentication Manager 支持的身份验证方法。

注意：Unix 服务器上允许的并发用户数量应针对每个工具、正在使用的操作系统，以及预期的并发服务器登录进行设置，特别是在使用 Cloud Authentication Service 时。

配置 telnet

配置 telnet 以提示用户选择 Cloud Authentication Service 和 RSA Authentication Manager 支持的身份验证方法。

过程

1. 切换到 **/etc** 目录。
2. 打开 **pam.conf** 文件，并滚动到 Authentication 部分。
3. 找到 telnet 部分，并注释下面一行：

   ```
   telnet auth required pam_aix
   ```

4. 添加与您要使用的 PAM 库的位版本匹配的行：

   对于 32 位：

   ```
   telnet auth required pam_securid.so
   ```

   对于 64 位：

   ```
   telnet auth required /opt/pam/lib/64bit/pam_securid.so
   ```

配置 login

配置 login 命令以提示用户使用 Cloud Authentication Service 和 RSA Authentication Manager 支持的身份验证方法。

过程

1. 切换到 **/etc** 目录
2. 打开 **pam.conf** 文件，并滚动到 Authentication 部分。
3. 找到 login 部分，并注释下面一行：

   ```
   login auth required pam_aix
   ```

4. 添加与您要使用的 PAM 库的位版本匹配的行：

   对于 32 位：

   ```
   login auth required pam_securid.so
   ```

对于 64 位：

```
login auth required /opt/pam/lib/64bit/pam_securid.so
```

配置 rlogin

配置 rlogin 应用工具以提示用户使用 Cloud Authentication Service 和 RSA Authentication Manager 支持的身份验证方法。

过程

1. 切换到 **/etc** 目录。
2. 打开 **pam.conf** 文件，并滚动到 Authentication 部分。
3. 找到 rlogin 部分，并注释下面一行：

   ```
   rlogin auth required pam_aix
   ```

4. 添加适合您正在配置的工具的位版本的行：

   对于 32 位：

   ```
   rlogin auth required pam_securid.so
   ```

   对于 64 位：

   ```
   rlogin auth required /opt/pam/lib/64-bit/pam_securid.so
   ```

配置 su

配置 su 命令以提示用户使用 Cloud Authentication Service 和 RSA Authentication Manager 支持的身份验证方法。

过程

1. 切换到 **/etc** 目录。
2. 打开 **pam.conf** 文件，并滚动到 Authentication 部分。
3. 找到 su 部分，并注释下面一行：

   ```
   su auth required pam_aix
   ```

4. 添加与您要使用的 PAM 库的位版本匹配的行：

   对于 32 位：

   ```
   su auth required pam_securid.so
   ```

   对于 64 位：

   ```
   su auth required /opt/pam/lib/64bit/pam_securid.so
   ```

配置 ssh 和相关工具

您可以配置 SSH 和相关工具，例如 scp 和 sftp，以提示用户使用 Cloud Authentication Service 和 RSA Authentication Manager 支持的身份验证方法。

过程

1. 切换到 **/etc** 目录。
2. 打开 **pam.conf** 文件。
3. 在 Authentication、Account Management、Password Management 和 Session Management 部分，注释掉下面一行的所有实例：

   ```
   OTHER <module_type> required pam_prohibit.
   ```

   其中 *<module_type>* 是 auth、account、password 或 session，具体取决于该行所在的部分。

4. 在 Account Management、Password Management 和 Session Management 部分添加下面一行：

   ```
   OTHER <module_type> required pam_aix
   ```

   其中 *<module_type>* 是 account、password 或 session。

5. 在 Authentication 部分中，注释下面一行：

   ```
   sshd auth required pam_aix
   ```

6. 添加适合您正在配置的工具的位版本的行：

   对于 32 位：

   ```
   sshd auth required pam_securid.so
   ```

   对于 64 位：

   ```
   sshd auth required /opt/pam/lib/64-bit/pam_securid.so
   ```

配置 sudo

如果您需要 sudo，则必须配置 sudo 命令以提示用户使用 Cloud Authentication Service 和 RSA Authentication Manager 支持的身份验证方法。

准备工作

从 https://www.sudo.ws 下载并安装受支持的 sudo 版本。

过程

1. 切换到 **/etc** 目录。
2. 打开 **pam.conf** 文件，并滚动到 Authentication 部分。
3. 找到 sudo 部分，并注释下面一行：

   ```
   sudo auth required pam_aix
   ```

4. 添加适合您正在配置的工具的位版本的行：

   对于 32 位：

   ```
   sudo auth required pam_securid.so
   ```

   对于 64 位：

   ```
   sudo auth required /opt/pam/lib/64-bit/pam_securid.so
   ```

配置 ftp

配置 ftp 协议，以提示用户使用 RSA Authentication Manager 支持的身份验证方法。

您不能使用 Cloud Authentication Service 保护 ftp；但可以使用 sftp。有关说明，请参阅配置 ssh 和相关工具 在本页 21。

过程

1. 切换到 **/etc** 目录。
2. 打开 **pam.conf** 文件，并滚动到 Authentication 部分。
3. 找到 ftp 部分，并注释下面一行：
   ```
   ftp auth required pam_aix
   ```
4. 添加适合您正在配置的工具的位版本的行：

   对于 32 位：

   ```
   ftp auth required pam_securid.so
   ```

   对于 64 位：

   ```
   ftp auth required /opt/pam/lib/64-bit/pam_securid.so
   ```

配置 dtlogin

您可以配置 dtlogin 以提示用户使用 Cloud Authentication Service 和 RSA Authentication Manager 支持的身份验证方法。

过程

1. 切换到 **/etc** 目录。
2. 打开 **pam.conf** 文件，并滚动到 Authentication Management 部分。
3. 找到 dtlogin 部分，并注释下面一行：
   ```
   dtlogin auth required pam_aix
   ```
4. 添加适合您正在配置的工具的位版本的行：
   对于 32 位：
   ```
   dtlogin auth required pam_securid.so
   ```
   对于 64 位：
   ```
   dtlogin auth required /opt/pam/lib/64-bit/pam_securid.so
   ```

第 2 章：配置功能

配置代理和 Unix 功能

您可以自定义 PAM Agent 配置以使用可选的代理和 UNIX 功能。

注意：在自定义代理之前，制作原始配置文件的备份副本。

要自定义代理，请参阅：

为 RSA Authentication Manager 启用代理报告 向下

启用调试输出 向下

为 UDP 模式启用 SecurID 跟踪日志记录 对页

配置可叠加的模块 对页

使用保留密码 在本页 27

启用选择性 SecurID 身份验证 在本页 27

配置指数退避时间 在本页 29

为 RSA Authentication Manager 启用代理报告

您可以在 **mfa_api.properties** 文件中配置 ENABLE_AGENT_REPORTING 参数，以便向 RSA Authentication Manager 发送代理的详细信息，如主机名、代理版本和操作系统版本。您可以使用 RSA Authentication Manager 8.3 运行报告，以包括这些详细信息。

准备工作

您必须在安装了代理的计算机上拥有 root 权限，并对存储 **mfa_api.properties** 文件的目录拥有写入权限。默认情况下，此文件存储在 **/var/ace/conf** 中。

过程

1. 切换到 **mfa_api.properties** 所在的目录。默认情况下，目录是 **/var/ace/conf**。
2. 打开 **mfa_api.properties**。
3. 将 ENABLE_AGENT_REPORTING 参数更改为 1，这将启用代理报告。默认值为 0。
4. 保存文件。

   PAM Agent 以及安装它的计算机的详细信息将包含在发送给 Authentication Manager 的 PAM Agent 报告详细信息中。

启用调试输出

为了进行故障排除，您可以对 PAM Agent 使用的特定工具启用调试输出。

您还可以配置系统日志以记录所有 PAM Agent 身份验证日志消息。有关更多信息，请参阅PAM Agent 的日志记录 在本页 38。

过程

1. 切换到位于 **/etc/** 目录中的配置文件 **pam.conf**。
2. 键入：

   ```
   tool name auth required pam_securid.so debug
   ```

   其中 *tool name* 是要启用调试输出的工具的名称。

对于 64 位工具，将 **pam_securid.so** 替换为完全限定路径 **/opt/pam/lib/64bit/pam_securid.so**。

为 UDP 模式启用 SecurID 跟踪日志记录

您可为 PAM Agent 以及身份验证应用工具 acetest 和 acestatus 启用详细的 SecurID 跟踪日志记录。默认情况下，当您安装 PAM Agent 时，SecurID 跟踪日志记录处于禁用状态。

过程

1. 切换到 **/etc/** 目录，并打开 **sd_pam.conf** 文件。
2. 要启用详细的代理日志记录并设置日志记录级别，请设置以下变量：

   RSATRACELEVEL=*value*

   其中 *value* 是下表中的设置。

值	描述
0	禁用日志记录(默认值)
1	记录常规消息
2	记录函数入口点
4	记录函数退出点
8	所有的逻辑流控制均使用此项 (ifs)

   对于组合，请添加相应的值。例如，要记录常规消息和函数入口点，请将该值设置为 3。

3. 指定日志重定向到的文件路径。设置以下变量：

   RSATRACEDEST=*filepath*

   其中 *filepath* 是文件路径。

   默认情况下，此变量为空。如果不设置此变量，则对于身份验证应用工具 acetest 和 acestatus，日志将转为标准错误，即使已指定 RSATRACELEVEL 值，也不会为身份验证工具生成日志。

4. 保存更改。

配置可叠加的模块

在堆叠配置中，可使用代理将 RSA SecurID PAM 身份验证模块与您环境中的其他 PAM 身份验证模块集成。密码或通行码从一个身份验证模块传递到下一个身份验证模块。您可以通过编辑 **/etc/pam.conf** 配置文件来配置身份验证质询的优先级。

注意：当堆叠配置与 Cloud Authentication Service 一起使用时，参数 use_first_pass 和 try_first_pass 不受支持。

代理使用参数 use_first_pass 和 try_first_pass：

- **use_first_pass。**代理仅使用从前一个模块传递的密码或通行码，如果凭证不匹配，则拒绝访问。不提示用户再次进行身份验证。
- **try_first_pass。**代理使用从上一个模块传递的密码或通行码。如果凭据不匹配，系统会提示用户进行身份验证。

注意：当从 SecurID 身份验证中排除的用户尝试通过登录访问 RSA PAM 模块但失败时，指数退避功能可确保 RSA PAM 模块保持控制权，直到登录成功或身份验证会话结束。有关配置指数退避时间的更多信息，请参阅配置指数退避时间 在本页 29。

以下部分提供了如何在堆叠环境中配置连接工具(登录工具) 的示例。

过程

1. 在 PAM Agent 主机计算机上，切换到 **/etc**，并打开 **pam.conf** 文件。
2. 添加下面几行。键入：

   ```
   login auth required pam_aix
   ```

   ```
   login auth required pam_securid.so
   ```

   对于 64 位工具，将 **pam_securid.so** 替换为完全限定路径 **/opt/pam/lib/64bit/pam_securid.so**。

使用保留密码

保留密码功能是一种紧急访问方法，使管理员无需输入 RSA SecurID 密码即可身份验证到安装了代理的受保护计算机。PAM Agent 只允许 root 管理员在不可预见的情况下(例如代理和 RSA Authentication Manager 之间的通信中断) 使用保留密码。在这些情况下，如果用户需要立即访问托管资源，管理员可以暂时禁用该代理。

注意：UNIX 密码是保留密码。

过程

打开 **pam.conf** 文件并键入：

```
tool name auth required pam_securid.so reserve
```

其中 *tool name* 是需要为其配置保留密码的工具的名称。对于 64 位工具，将 **pam_securid.so** 替换为完全限定路径 **/opt/pam/lib/64bit/pam_securid.so**。

启用选择性 SecurID 身份验证

您可以配置代理以选择性地始终或从不提示特定的 UNIX 用户或组进行 SecurID 身份验证：

为 UNIX 组启用选择性 SecurID 身份验证 对页

为 UNIX 用户启用选择性 SecurID 身份验证 对页

注意：当同时启用选择性组支持和选择性用户支持时，将仅启用选择性用户支持，并忽略选择性组支持。

下表列出了可以在 **sd_pam.conf** 文件中设置的可能的值。

ENABLE_ GROUPS_ SUPPORT	ENABLE_ USERS_ SUPPORT	结果
0	0	两项功能均未启用。每个用户和用户组都将接受质询。
0	1	启用所选用户支持。 PAM Agent 始终提示特定 UNIX 用户使用 SecurID 进行身份验证，或者从不提示特定用户使用 SecurID 进行身份验证。
1	0	启用所选组支持。 PAM Agent 始终提示特定 UNIX 组使用 RSA SecurID 进行身份验证，或者从不提示特定组使用 SecurID 进行身份验证。
1	1	启用所选用户支持。 PAM Agent 始终提示特定 UNIX 用户使用 SecurID 进行身份验证，或者从不提示特定用户使用 SecurID 进行身份验证。

为 UNIX 组启用选择性 SecurID 身份验证

您可以将 PAM Agent 配置为始终或从不提示特定 UNIX 组使用 RSA SecurID 进行身份验证。如果安装了 PAM Agent，则不启用此功能。

从 SecurID 身份验证中排除的组成员可以使用 UNIX 凭据或通过堆栈中的另一个 PAM 模块进行身份验证。要执行此操作，请配置 PAM_IGNORE_SUPPORT 参数。

注意：不要指定 RSA Authentication Manager 组。此功能仅适用于 UNIX 组。

过程

1. 切换到 **/etc** 目录，并打开 **sd_pam.conf** 文件。
2. 将 ENABLE_GROUP_SUPPORT 参数设置为 1。默认值为 0。
3. 填充 LIST_OF_GROUPS 参数。
4. 设置 INCL_EXCL_GROUPS 参数的值。
   有效值包括：
   0 — 对列出的组禁用 SecurID 身份验证（默认值）。
   1 — 仅对列出的组启用 SecurID 身份验证。
5. （可选）设置 PAM_IGNORE_SUPPORT 参数。
   有效值包括：
   0 — 启用 UNIX 密码身份验证（默认值）。
   1 — 禁用 UNIX 密码身份验证。
   此参数仅适用于从 SecurID 身份验证过程中排除的组。
6. 保存文件。

为 UNIX 用户启用选择性 SecurID 身份验证

您可以将 PAM Agent 配置为始终或从不提示特定 UNIX 用户使用 SecurID 进行身份验证。如果安装了 PAM Agent，则不启用此功能。

从 SecurID 身份验证中排除的用户可以使用 UNIX 凭据或通过堆栈中的另一个 PAM 模块进行身份验证。要执行此操作，请配置 PAM_IGNORE_SUPPORT_FOR_USERS 参数。

过程

1. 切换到 **/etc** 目录，并打开 **sd_pam.conf** 文件。
2. 将 ENABLE_USERS_SUPPORT 参数设置为 1。默认值为 0。
3. 填充 LIST_OF_USERS 参数。
4. 设置 INCL_EXCL_USERS 参数的值。
   有效值包括：
   0 — 对列出的用户禁用 SecurID 身份验证（默认值）。
   1 — 仅对列出的用户启用 SecurID 身份验证。
5. （可选）设置 PAM_IGNORE_SUPPORT_FOR_USERS 参数。
   有效值包括：
   0 — 启用 UNIX 密码身份验证（默认值）。
   1 — 禁用 UNIX 密码身份验证。
   此参数仅适用于从 SecurID 身份验证过程中排除的用户。
6. 保存文件。

配置指数退避时间

您可以配置从 RSA SecurID 身份验证中排除的用户在每次连续失败登录尝试后进行身份验证之前需要等待的时间。默认情况下，用户可以在登录尝试失败后重试 UNIX 身份验证，延迟时间为 pow(4, failattempts) 秒。例如，三次失败的登录尝试导致 64 秒延迟(四的三次幂，即 4 X 4 X 4 = 64) 。

注意：ftp 协议不支持指数退避延迟。

过程

1. 切换到 **/etc** 目录，并打开 **sd_pam.conf** 文件。
2. 将 BACKOFF_TIME_FOR_RSA_EXCLUDED_UNIX_USERS 参数设置为 *N*，如下所示：

N	**身份验证行为**
0	登录尝试失败后禁林重试 UNIX 身份验证。登录尝试失败后，立即重试身份验证，没有延迟。
1,2,3	允许在登录尝试失败后重试 UNIX 身份验证，延迟时间为 pow(3, failattempts) 秒。
4	允许在登录尝试失败后重试 UNIX 身份验证，延迟时间为 pow(4, failattempts) 秒。
5/Above	允许在登录尝试失败后重试 UNIX 身份验证，延迟时间为 pow(5/Above, failattempts) 秒。

更改 PAM Agent 身份验证模式

您可以更改 PAM Agent 的身份验证模式。例如，如果您想使用 Cloud Authentication Service 提供的扩展身份验证选项，则可以更改模式。默认情况下，升级后的 PAM Agent 将 RSA Authentication Manager 与 UDP 协议结合使用。

从 UDP 协议更改为 REST 协议

您可以针对 RSA Authentication Manager 或 Cloud Authentication Service 将 UDP 协议身份验证模式更改为 REST 协议。

准备工作

- 在安装代理的计算机上，您必须具有根权限。
- 您必须对存储 **sdconf.rec** 文件的目录拥有写入权限。默认情况下，此文件存储在 **/etc** 中。
- 您必须对存储 **mfa_api.properties** 文件的目录拥有写入权限。默认情况下，此文件存储在 **/var/ace/conf** 中。
- 收集必要的信息。

  对于采用 REST 协议的 Authentication Manager 身份验证，要求您的 Authentication Manager 超级管理员提供以下信息。

参数	**描述**
REST_URL	身份验证代理和 Authentication Manager 主实例之间的通信的 REST 服务器 URL。例如，https://*HOSTNAME*:*PORT_NO*/mfa/v1_1/authn
REPLICA_*number* 其中，*number* 是 1	可用于故障切换的每个复制副本实例的 REST 服务器 URL。例如，https://*HOSTNAME*:*PORT_NO*/mfa/v1_1/authn

参数	描述
到 15 之间的数字。	
CLIENT_KEY	用于安全地将用户身份验证请求传递给 Authentication Manager 的访问密钥（客户端密钥）。该值在 Authentication Manager 主实例的安全控制台中生成。
CA_CERT_FILE_PATH	在身份验证代理上，服务器受信任证书的目录和文件名。默认值是 **/var/ace/cert.pem**。
CLIENT_ID	在 Authentication Manager 中为 PAM Agent 创建的身份验证代理名称（客户端 ID）。

对于采用 Cloud Authentication Service 的身份验证，要求您的 Cloud Authentication Service 超级管理员提供以下信息：

参数	描述
REST_URL	代理与 Cloud Authentication Service 之间的通信的 REST 服务器 URL。例如，https://*HOSTNAME*:*PORT_NO*/mfa/v1_1/authn
CLIENT_KEY	在 Cloud Administration Console 中创建的身份验证 API 密钥（客户端密钥），用于安全地将用户身份验证请求传递给 Cloud Authentication Service。
CA_CERT_FILE_PATH	在身份验证代理上，输入服务器可信证书的目录和文件名。默认值是 **/var/ace/cert.pem**。
TENANT_ID	Cloud Authentication Service 的租户 ID。PAM Agent 可以在身份验证请求中提供租户 ID，但代理不会验证该数据。Cloud Authentication Service 目前不支持此参数。
ASSURANCE_POLICY_ID	Cloud Authentication Service 的访问策略名称。
CLIENT_ID	要显示在移动通知中的身份验证代理名称。您可以输入任何值。例如，PAM_Agent。

过程

1. 切换到 **sd_pam.conf** 所在的目录。默认位置为 **/etc**。
2. 打开 **sd_pam.conf**。
3. 更改 OPERATION_MODE 参数：
   - 对于采用 REST 协议的 Authentication Manager，输入 1。
   - 对于采用 REST 协议的 Cloud Authentication Service，输入 2。

   如果 OPERATION_MODE 参数为 0、未指定或已注释掉，则 PAM Agent 默认为 UDP 模式。
4. 切换到目录 **/var/ace/conf**。您需要更新 **mfa_api.properties** 文件。
5. 打开 **mfa_api.properties**。
6. 删除注释，以启用所需的参数。
7. 为每个必需的参数输入一个值。
8. 保存文件。

   您现在可以使用 REST 协议。

从 REST 协议更改为 UDP 协议

在安装 PAM Agent 以使用 REST 协议后，您可以更改身份验证模式，以便将 RSA Authentication Manager 与 UDP 协议结合使用。

将身份验证模式更改为使用 UDP 协议后，**mfa_api.properties** 文件中的 REST 协议配置设置不再适用。

准备工作

- Authentication Manager 配置文件 **sdconf.rec** 是必需的。您可以在 Authentication Manager 中生成此文件，也可以从您的 Authentication Manager 超级管理员处获取此文件。有关详细信息，请参阅规划 PAM Agent 的安装 在本页 13。
- 您必须在安装了代理的计算机上拥有根权限，并对存储 **sd_pam.conf** 文件的目录拥有写入权限。默认情况下，此文件存储在 **/etc** 目录中。

过程

1. 切换到 **sd_pam.conf** 所在的目录。默认位置为 **/etc**。
2. 打开 **sd_pam.conf**。
3. 将 OPERATION_MODE 参数更改为 0 以使用 UDP 协议：

   ```
   OPERATION_MODE=0
   ```

   如果 OPERATION_MODE 参数为 0、未指定或已注释掉，则 PAM Agent 默认为 UDP 模式。

4. 将 **sdconf.rec** 拷贝到 **/var/ace** 目录中。

   您现在可以使用 UDP 协议。

在 RSA Authentication Manager 和 Cloud Authentication Service 之间更改

您可以更改 PAM Agent 是将 REST 协议与 Authentication Manager 还是 Cloud Authentication Service 结合使用。

准备工作

- 在安装代理的计算机上，您必须具有根权限。
- 您必须对存储 **sdconf.rec** 文件的目录拥有写入权限。默认情况下，此文件存储在 **/var/ace** 中。
- 您必须对存储 **mfa_api.properties** 文件的目录拥有写入权限。默认情况下，此文件存储在 **/var/ace/conf** 中。
- 服务器受信任证书的参数 CA_CERT_FILE_PATH 可以保持不变。对于其他参数，收集所需的信息：
  对于采用 REST 协议的 Authentication Manager 身份验证，要求您的 Authentication Manager 超级管理员提供以下信息：

参数	描述
REST_URL	身份验证代理和 Authentication Manager 主实例之间的通信的 REST 服务器 URL。例如，https://*HOSTNAME*:*PORT_NO*/mfa/v1_1/authn
REPLICA_*number* 其中，*number* 是 1 到 15 之间的数字。	可用于故障切换的每个复制副本实例的 REST 服务器 URL。例如，https://*HOSTNAME*:*PORT_NO*/mfa/v1_1/authn
CLIENT_KEY	用于安全地将用户身份验证请求传递给 Authentication Manager 的访问密钥（客户端密钥）。该值在 Authentication Manager 主实例的安全控制台中生成。
CLIENT_ID	在 Authentication Manager 中为 PAM Agent 创建的身份验证代理名称（客户端 ID）。

对于采用 Cloud Authentication Service 的身份验证，向您的 Cloud Authentication Service 超级管理员询问以下信息：

参数	描述
REST_URL	代理与 Cloud Authentication Service 之间的通信的 REST 服务器 URL。例如，https://*HOSTNAME*:*PORT_NO*/mfa/v1_1/authn

参数	描述
CLIENT_KEY	在 Cloud Administration Console 中创建的身份验证 API 密钥（客户端密钥），用于安全地将用户身份验证请求传递给 Cloud Authentication Service。
TENANT_ID	Cloud Authentication Service 的租户 ID。PAM Agent 可以在身份验证请求中提供租户 ID，但代理不会验证该数据。Cloud Authentication Service 目前不支持此参数。
ASSURANCE_POLICY_ID	Cloud Authentication Service 的访问策略名称。
CLIENT_ID	要显示在移动通知中的身份验证代理名称。您可以输入任何值。例如，PAM_Agent。

过程

1. 切换到 **sd_pam.conf** 所在的目录。默认位置为 **/etc**。
2. 打开 **sd_pam.conf**。
3. 更改 OPERATION_MODE 参数：
   - 对于采用 REST 协议的 Authentication Manager，输入 1。
   - 对于采用 REST 协议的 Cloud Authentication Service，输入 2。

   如果 OPERATION_MODE 参数为 0、未指定或已注释掉，则 PAM Agent 默认为 UDP 模式。
4. 切换到目录 **/var/ace/conf**。您必须更新 **mfa_api.properties** 文件中各参数的必需值。
5. 打开 **mfa_api.properties**。
6. 删除注释以启用必需的参数，并注释掉不再需要的任何参数。
7. 为每个必需的参数输入一个值。
8. 保存文件。

   现在您可以将 REST 协议与新身份验证模式结合使用。

附录 A：故障排除

已知配置问题

本部分描述了已知问题。

支持的工具的问题

工具	已知问题
dtlogin	**问题：**显示限制可能会导致用户遇到两个问题： • 进行身份验证的用户无法看到有关可用身份验证方法的全部消息。 • 保留密码用户可以在屏幕上看到不需要的部分文本输入字段。 **解决方案：**进行身份验证的用户可以按照屏幕上的指示按 Enter，以查看完整消息。保留密码用户可以忽略不必要的字段。
ftp	• **问题：**当您使用 SecurID 保护 ftp 时，不向用户显示 SecurID 身份验证提示和错误消息。只显示标准操作系统 (OS) 提示和错误消息。 **解决方案：** 指示用户在操作系统用户名提示处输入用户名，并在操作系统密码提示处输入 SecurID 通行码。 如果用户不知道令牌状态(例如，令牌处于"下一个令牌码"模式或"新 PIN"模式) ，则用户必须使用另一个连接工具(如 rlogin) 进行身份验证，以验证 PIN 或令牌码仍然有效。 • FTP 不支持指数级退避延迟。 • 您不能使用 Cloud Authentication Service 保护 ftp；但支持 sftp。
ssh	**问题：**用户在单个会话中进行三次不成功的 SecurID 身份验证尝试后，连接将关闭。 **解决方案：** 用户可以终止该会话，并启动另一个会话。
rlogin、telnet	**问题：**使用 REST 协议进行身份验证时，系统不会提示输入错误登录信息的用户再次输入其凭据，而是关闭连接。 **解决方案：** 通过注释 **/var/ace/conf/log.properties** 中所有可用的附加器，禁用 REST 日志记录。

升级和卸载问题

问题：如果您尝试升级或卸载 PAM Agent 而没有禁用 RSA PAM 模块，您可能会收到错误消息："pam_securid.so 正忙，无法删除/替换。"

解决方案：要解决升级过程中的此问题，请运行以下命令以重新启动升级过程：
`/usr/sbin/slibclean`

要解决卸载 PAM Agent 时的这一问题，您必须使用 ssh 以外的工具登录，并手动删除 **pam_securid.so**。

UDP 模式的身份验证应用工具

身份验证应用工具位于以下目录中：

- 32 位操作系统：***pam agent 安装目录*/bin/32bit**
- 64 位操作系统：***pam agent 安装目录*/bin/64bit**

使用这些应用工具执行以下操作：

- 执行测试身份验证。有关详细信息，请参阅 运行 acetest 应用工具 向下。
- 验证 PAM Agent 和 RSA Authentication Manager 之间的通信。有关详细信息，请参阅 运行 acestatus 应用工具 向下。

您可以启用这些应用工具的日志记录。有关详细信息，请参阅为 UDP 模式启用 SecurID 跟踪日志记录 在本页 26。

运行 acetest 应用工具

此应用工具通过执行测试身份验证，来检查代理是否正常工作。

过程

1. 切换到 PAM Agent 身份验证应用工具目录。
   - 32 位操作系统：***pam agent 安装目录*/bin/32bit**
   - 64 位操作系统：***pam agent 安装目录*/bin/64bit**
2. 键入：

   ```
   ./acetest
   ```

3. 输入有效用户名和密码。

如果您被反复拒绝访问，请使用 运行 acestatus 应用工具 向下 应用工具测试与 Authentication Manager 服务器的连接，或联系您的 Authentication Manager 管理员。

运行 acestatus 应用工具

此应用工具检查其中的 PAM Agent 注册为代理主机的每个 Authentication Manager 的状态。如果您对所显示的信息有疑问，请联系您的 Authentication Manager 管理员。

过程

1. 切换到 PAM Agent 应用工具目录。
2. 键入：

   ```
   ./acestatus
   ```

下表列出了 Authentication Manager 部分中显示的信息。

返回的信息	描述
配置版本	正在使用中的 **sdconf.rec** 文件的版本。对于 RSA Authentication Manager 8.0 或更高版本，此数字为 14。
DES 已启用	如果您的配置环境支持传统协议，则显示 YES。
客户端重试次数	在发生超时之前，PAM Agent 向 Authentication Manager 发送身份验证数据的次数。
客户端超时	PAM Agent 在向 Authentication Manager 重新发送身份验证数据之前等待的时间(以秒为单位) 。
服务器版本	Authentication Manager 的版本号。
通信	Authentication Manager 和 PAM Agent 使用的协议版本。

下表列出了 Authentication Manager 部分中显示的状态信息。

状态信息	描述
服务器活动地址	PAM Agent 用于与服务器通信的 IP 地址。该地址可能是您选择的服务器的实际 IP 地址，也

状态信息	描述
	可能是分配给服务器的别名 IP 地址。IP 地址 0.0.0.0 表示代理尚未接收到来自服务器的通信。

下表列出了 Authentication Manager 部分中显示的服务器状态信息。

服务器状态	描述
可用于进行身份验证	此服务器可以处理身份验证请求。
未使用	此服务器尚未收到身份验证请求。
仅用于故障切换	此服务器保留用于故障切换。
初始请求期间的默认服务器	目前只有此服务器可以处理请求。

UDP 模式的转换应用工具

当基于 UDP 的 PAM Agent 与其他 SecurID 代理共存时，可使用转换应用工具。

转换应用工具 ns_conv_util 位于以下目录中：

- 32 位操作系统：***pam agent home*/bin/32bit**
- 64 位操作系统：***pam agent home*/bin/64bit**

过程

1. 切换到 PAM Agent 应用工具目录。
2. 键入：

   ```
   ./ns_conv_util <Existing_Securid_file_path> <New_Securid_dir_path>
   ```

   其中 *<Existing_Securid_file_path>* 是当前 SecurID 文件所在的路径，

   <New_Securid_dir_path> 是存储新生成的 SecurID 文件的目录。

   例如：

   ```
   ./ns_conv_util /var/ace/securid /var/ace_pam/
   ```

3. 如果新的目标位置不是 VAR_ACE 指定的位置，则将新的 SecurID 文件拷贝到此位置。

UDP 模式的节点密码

节点密码是一个对称加密密钥，由 RSA Authentication Manager 和 PAM Agent 用于在数据包在网络中传输期间加密和解密数据包。使用 UDP 协议的代理都需要节点密码。共享节点密码同时存储在 Authentication Manager 数据库和安装 PAM Agent 的计算机上的文件中。使用 REST 协议的代理不需要节点密码文件，因为它不使用节点密码，而是使用一个动态协商的密钥与一个强加密算法来加密该信道。

对于基于 UDP 的代理，如果 Authentication Manager 服务器或安装 PAM Agent 的计算机上缺少节点密码，请清除另一个位置的节点密码。如果 Authentication Manager 和 PAM Agent 计算机上的节点密码文件不匹配，请清除两个位置中的节点密码。清除节点密码后，您必须生成新的节点密码。

从 RSA Authentication Manager 清除节点密码

如果 RSA Authentication Manager 上和安装 PAM Agent 的计算机上的节点密码不匹配，或者 PAM Agent 计算机上缺少节点密码，则必须清除 Authentication Manager 中的节点密码。例如，如果您重新安装 PAM Agent，PAM Agent 计算机上将缺少节点密码。

过程

1. 在 Authentication Manager 安全控制台中，单击**访问 > 身份验证代理 > 管理现有项**。
2. 查找受影响的代理计算机，然后从下拉菜单中选择**管理节点密码**。
3. 选择**清除节点密码**复选框，然后单击**保存**。

完成之后

- 如果 PAM Agent 计算机上没有节点密码，请参阅清除 PAM Agent 计算机上的节点密码 向下。
- 如果 PAM Agent 计算机没有节点密码，请执行此过程：生成新的节点密码 向下。

清除 PAM Agent 计算机上的节点密码

如果 RSA Authentication Manager 实例上和安装 PAM Agent 的计算机上的节点密码不匹配，或者 Authentication Manager 中缺少节点密码，则必须清除 PAM Agent 计算机中的节点密码。例如，如果您安装新 Authentication Manager 实例，并添加现有 PAM Agent，则 Authentication Manager 中将缺少节点密码。

准备工作

如果 Authentication Manager 上没有节点密码，请参阅从 RSA Authentication Manager 清除节点密码 向上。

过程

1. 登录到安装 PAM Agent 的计算机，然后找到 **/var/ace** 目录中的节点密码文件 **securid**。
2. 重命名或删除节点密码文件。
3. 节点密码还存储在服务器缓存中。重新启动计算机以清除缓存中的节点密码。

完成之后

生成新的节点密码 向下

生成新的节点密码

过程

1. 从 PAM Agent 计算机运行 acetest 应用工具以生成节点密码文件。有关详细信息，请参阅UDP 模式的身份验证应用工具 在本页 35。
2. 检查您的身份验证日志，并确保新的节点密码已发送。
3. 重新启动 PAM Agent 计算机，以便代理可以读取节点密码文件。

PAM Agent 的日志记录

如果启用日志记录，默认情况下，PAM Agent 身份验证消息记录在系统日志中。为了进行跟踪，您可以将系统日志配置为记录特定工具的 PAM Agent 身份验证日志消息。请参阅启用调试输出 在本页 25。

为 AIX 配置系统日志

以下过程将所有身份验证消息发送到系统日志。

过程

1. 切换到 **/etc** 目录。
2. 打开 **syslog.conf** 文件。
3. 向指定系统日志文件的行添加 auth.notice 参数。
4. 删除 authpriv.none 参数，如果为系统日志文件指定了该参数。
5. 如果使用 telnet 或 login，请向指定系统日志文件的行添加 authpriv.notice 参数。
6. 保存更改。
7. 重新启动 syslog 守护程序。

PAM Agent 身份验证日志消息

下表列出身份验证日志消息。

消息	描述
Cannot locate **sd_pam.conf** file	**/etc** 目录中不存在配置文件 **sd_pam.conf**；**/etc** 必须包含正确的配置文件，以便可以正确设置 VAR_ACE。
AceInitialize failed	AceInitialize 是一个 API 函数调用，用于初始化工作线程，并从 **sdconf.rec** 中加载配置设置。确认您已从 Authentication Manager 管理员处获得 **sdconf.rec** 的最新副本，并且 VAR_ACE 已正确设置。
Cannot communicate with RSA ACE/Server	任一 Authentication Manager 代理未启动，或者出现网络故障。联系您的 Authentication Manager 管理员或网络管理员。
Reserve password exceeds character limit	最大字符限制为 256 个字符。
Invalid reserve password	保留密码与主机的系统密码相同。如果 Authentication Manager 无法处理身份验证请求，则您必须知道此密码。
User name exceeds character limit	用户名不能超过 31 个字符。
Reserve password not allowed. User is not root.	确认您是 root 用户。只有 root 用户可以使用保留密码。

REST 模式的日志记录

REST 模式支持使用 **log4cxx** 库实施的其他日志记录。REST 层日志记录与 PAM Agent 日志是分开的。支持 RollingFileAppender 和 SyslogAppender。默认情况下，启用 RollingFileAppender。日志将记录到 **/var/ace/log/mfa_rest.log**，日志级别设置为 INFO。启用基于大小的轮换，轮换大小为 10 MB。

不支持基于时间的日志轮换。支持的工具(如 ssh 和 su) 会为每个请求加载身份验证代理，因此 PAM Agent 不能基于时间轮换日志。PAM Agent 支持基于大小的日志轮换。

可以更改 REST 模式的默认日志设置。

过程

1. 切换到 **/var/ace/conf** 目录。
2. 打开 **log.properties** 文件。

3. 为基于大小的轮换配置以下条目：

```
log4j.rootLogger=INFO, RestLogger

log4j.appender.RestLogger=org.apache.log4j.RollingFileAppender

log4j.appender.RestLogger.File=/var/ace/log/mfa_rest.log

log4j.appender.RestLogger.MaxFileSize=10MB

log4j.appender.RestLogger.MaxBackupIndex=10

log4j.appender.RestLogger.layout=org.apache.log4j.PatternLayout

log4j.appender.RestLogger.layout.ConversionPattern=%d [%t] %-5p
(%F:%L) - %m%n

log4j.appender.RestLogger.Append=true

log4j.appender.RestLogger.ImmediateFlush=true
```

4. 配置以下条目以支持本地和远程记录到 syslog：

```
log4j.rootLogger=INFO,Syslog

log4j.appender.Syslog=org.apache.log4j.net.SyslogAppender

log4j.appender.Syslog.syslogHost=localhost

log4j.appender.Syslog.Facility=DAEMON

log4j.appender.Syslog.layout=org.apache.log4j.PatternLayout

log4j.appender.Syslog.layout.ConversionPattern=%d{yyyy-MM-dd
HH:mm:ss:SSS}%p [%c] %m%n
```

5. 保存更改。
6. 重新启动 syslog 守护程序。

配置 REST 身份验证的超时和重试值

您可以配置 PAM Agent 连接到 RSA Authentication Manager 或 Cloud Authentication Service 所用时间，以及 PAM Agent 等待响应所用时间。您还可以配置 PAM Agent 尝试联系 Authentication Manager 主实例或复制副本实例或 Cloud Authentication Service 的次数。这些参数仅供 REST 协议使用。

请务必考虑您的网络速度。在较慢的网络上设置高超时值可使身份验证成功。

准备工作

您必须在安装了代理的计算机上拥有 root 权限，并对存储 **mfa_api.properties** 文件的目录拥有写入权限。默认情况下，此文件存储在 **/var/ace/conf** 中。

过程

1. 切换到 **mfa_api.properties** 所在的目录。默认情况下，目录是 **/var/ace/conf**。
2. 打开 **mfa_api.properties**。
3. 可以更改下列参数：
   - CONNECT_TIMEOUT。允许代理连接到服务器的最大秒数。默认值是 60 秒。
   - READ_TIMEOUT。允许连接到服务器并读取响应的最大秒数。READ_TIMEOUT 值必须等于 CONNECT_TIMEOUT 值与读取响应所允许的最长时间之和。默认值为 120 秒。
   - MAX_RETRIES。PAM Agent 尝试连接到 Authentication Manager 或 Cloud Authentication Service 的次数。默认值为 3。
   - 对于 Authentication Manager REST 接口的初始化阶段，当 PAM Agent 启动身份验证尝试时，MAX_RETRIES 是代理在故障切换到另一台服务之前尝试联系同一台服务器的次数。在验证阶段，当 PAM Agent 提供身份验证凭据时，不支持故障切换，并且 MAX_RETRIES 是代理在身份验证失败之前尝试联系同一台服务器的次数。
   - Cloud Authentication Service 不支持故障切换。对于初始化和验证阶段，MAX_RETRIES 是代理在身份验证失败之前尝试联系同一台服务器的次数。
4. 保存文件。

卸载 RSA SecurID Authentication Agent 8.0 for PAM

您可以手动卸载单个计算机上的 PAM Agent，也可以选择以静默方式自动卸载 PAM Agent 的多个副本。

准备工作

- 将 RSA SecurID 保护的工具配置为使用随操作系统提供的标准 PAM 模块，而不是 RSA PAM 模块。在继续卸载之前，必须先关闭使用 RSA PAM 模块的任何活动会话。您必须撤消在配置工具 在本页 19中执行的步骤。

  注意：如果在 **pam.conf** 文件中引用了 RSA 模块时卸载 RSA 模块，则您将被锁定在系统之外。

- 确认您在主机上拥有 root 权限。

从一台计算机上卸载 PAM Agent

执行此任务可卸载一个 PAM Agent。

过程

1. 切换到 PAM Agent 主目录。例如，**/opt/pam**。
2. 运行卸载脚本。键入：

   ```
   ./uninstall_pam.sh
   ```

3. 确认已删除安装目录。如果目录仍然存在，您必须手动将其删除。
4. 要验证 PAM Agent 是否已成功删除，请检查 **/var/pam_uninstaller/uninstaller.log** 文件。

在静默模式下批量卸载 PAM Agent

执行此任务以卸载大量 PAM Agent。

过程

1. 使用名称 **unconfig** 创建一个基于文本的配置文件。此文件包含以下信息：

   ```
   /opt/
   y
   y
   y
   ```

   其中 */opt/* 是 PAM Agent 的根路径，通常是 **/opt/**。

   对每个提示均响应 y：

   - Are you sure that you would like to uninstall the RSA Authentication Agent 8.0.0 [101] for PAM?
   - The RSA Authentication Agent for PAM will be deleted from the */opt* directory. Ok?
   - If you uninstall the RSA module while there are references to the RSA module in the PAM configuration file (file **pam.conf** or inside the directory **pam.d**), you will be locked out of your system. Proceed with uninstall? Ok?

2. 切换到 PAM Agent 主目录。例如，**/opt/pam**。

3. 运行卸载脚本。键入：

```
./uninstall_pam.sh < unconfig
```

附录 B：关键配置文件

关键配置文件

默认 PAM Agent 安装目录是 **/opt/pam**，这可在安装期间更改。默认情况下，**/var/ace** 目录包括 REST 相关库和文件。此目录位置无法更改。

除了二进制文件（**pam_securid.so**、**acetest**、**acestatus** 和 **ns_conv_util**），PAM Agent 还维护下表中列出的关键配置文件。

文件	描述
log.properties	REST 协议的 PAM Agent 日志记录配置文件。 PAM Agent 对 REST 模式日志记录使用库 **log4cxx**。
mfa_ api.properties	包含 REST 协议用于向 Authentication Manager 和 Cloud Authentication Service 进行身份验证的设置。
sdconf.rec	此文件由 RSA Authentication Manager 生成，并包含用于控制 PAM Agent 行为的配置信息。此文件的权限应为 -rw------- root root。 此文件仅在 UDP 模式下使用。
sdopts.rec	此文件用于手动负载平衡。它包含 Authentication Manager 实例的 IP 地址列表。此文件的权限应为 -rw------- root root。 此文件仅在 UDP 模式下使用。
sdstatus.12	此文件由 PAM Agent 身份验证 API 生成，以跟踪 Authentication Manager 服务器的上一个已知状态。此文件的权限应为 -rw------- root root。
sd_pam.conf	包含控制 PAM Agent 行为的配置设置。此文件的权限应为 -rw-r--r-- root root。
securid	此文件包含一个共享密钥，用来保护本地计算机和 Authentication Manager 之间的 UDP 协议通信。此文件的名称来源于本地系统为代理与 Authentication Manager 通信的端口配置的协议名称（通常通过“services”文件）。此文件的权限应为 -r-------- root root。不过，它还取决于操作系统 Umask 设置。 UDP 协议需要此文件。此文件对使用 REST 协议的身份验证是可选的。