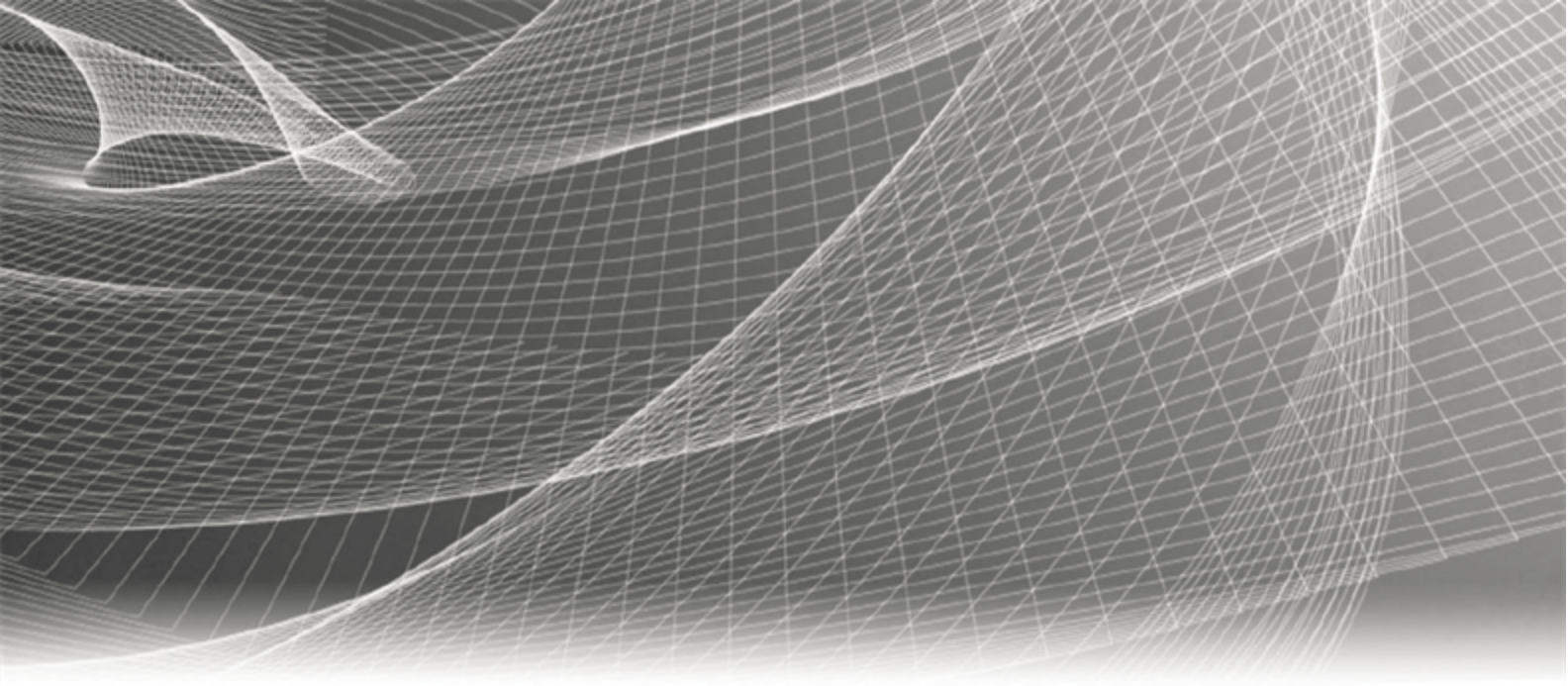

RSA SECURID® ACCESS

RSA® Authentication Agent 8.1 for PAM

Guia de Instalação e Configuração para Oracle e RHEL

Informações de contato

Este link da RSA, https://community.rsa.com, contém uma base de conhecimento que responde a perguntas comuns e fornece soluções para problemas conhecidos, documentação do produto, discussões da comunidade e gerenciamento de casos.

Marcas comerciais

Dell, RSA, o logotipo da RSA, EMC e outras marcas comerciais são marcas comerciais da Dell Inc. ou de suas subsidiárias. Outras marcas comerciais podem ser marcas comerciais de seus respectivos proprietários. Para obter uma lista das marcas comerciais da RSA, acesse brazil.emc.com/legal/emc-corporation-trademarks.htm.

Contrato de Licença

Este software e a documentação associada são propriedade particular e confidencial da Dell Inc. ou de suas subsidiárias, são fornecidos sob licença e só podem ser usados e copiados nos termos dessa licença e com a inclusão do aviso de direitos autorais abaixo. Este software e a documentação, bem como quaisquer cópias destes, não podem ser fornecidos nem disponibilizados por qualquer outra pessoa.

Nenhuma posse ou propriedade do software ou da documentação ou nenhuma propriedade intelectual relacionada será transferida por meio do presente instrumento. Qualquer uso ou reprodução não autorizada deste software e da documentação estará sujeito a responsabilidade civil e/ou criminal.

Este software está sujeito a alteração sem prévio aviso e não deve ser interpretado como um compromisso da Dell Inc.

Licenças de terceiros

Este produto pode incluir software desenvolvido por outros parceiros além da RSA. O texto dos contratos de licença, aplicáveis a software de terceiro neste produto, pode ser visualizado na página de documentação do produto no link da RSA. Ao utilizar esse produto, o usuário concorda totalmente com os termos dos contratos de licença.

Observação sobre as tecnologias de criptografia

Este produto pode conter tecnologia de criptografia. Muitos países proíbem ou restringem o uso, a importação ou a exportação de tecnologias de criptografia, e as normas vigentes de uso, importação e exportação devem ser seguidas ao usar, importar ou exportar este produto.

Distribuição

O uso, a cópia e a distribuição de qualquer software da DELL descrito nesta publicação exigem uma licença de software.

A Dell Inc. assegura que as informações apresentadas neste documento estão corretas na data da publicação. As informações estão sujeitas a alterações sem prévio aviso.

AS INFORMAÇÕES CONTIDAS NESTA PUBLICAÇÃO SÃO FORNECIDAS "NO ESTADO EM QUE SE ENCONTRAM". A DELL INC. NÃO OFERECE REPRESENTAÇÕES NEM GARANTIAS DE NENHUM TIPO NO QUE SE REFERE ÀS INFORMAÇÕES CONTIDAS NESTA PUBLICAÇÃO, ASSIM COMO SE ISENTA ESPECIFICAMENTE DE GARANTIAS IMPLÍCITAS DE COMERCIALIZAÇÃO OU ADEQUAÇÃO A UMA FINALIDADE ESPECÍFICA.

Outubro de 2018

Índice

Prefácio

Público-alvo

Este guia destina-se aos administradores de rede e sistema que instalam, fazem upgrade e solucionam problemas do RSA® Authentication Agent for PAM (módulo de autenticação conectável).

Suporte e serviço

Você pode acessar a comunidade e obter informações de suporte neste link da RSA https://community.rsa.com. Esse link da RSA contém uma base de conhecimento que responde a perguntas comuns e fornece soluções para problemas conhecidos, documentação de produto, discussões da comunidade e gerenciamento de casos.

Programa de parceiros RSA Ready

O site do programa de parceria RSA Ready, em www.rsaready.com, apresenta informações sobre produtos de hardware e software de terceiros que foram certificados para funcionar com produtos RSA. O site inclui guias de implementação com instruções detalhadas e outras informações sobre a interoperação dos produtos RSA com produtos de terceiros.

Capítulo 1: Instalando o PAM Agent

Visão geral do RSA Authentication Agent 8.1 for PAM

O RSA Authentication Agent 8.1 for PAM (módulo de autenticação conectável) comporta a autenticação em sistemas UNIX com ferramentas de conexão padrão ou OpenSSH. O PAM agent usa bibliotecas personalizadas compartilhadas da RSA e dá suporte ao acesso a servidores e estações de trabalho UNIX com os métodos de autenticação compatíveis com o Serviço de autenticação da nuvem e o RSA Authentication Manager.

Você pode escolher se o PAM agent será autenticado no Serviço de autenticação da nuvem ou no Authentication Manager. A licença do RSA SecurID Access Enterprise Edition e a licença do Premium Edition incluem esses dois componentes do RSA SecurID Access. O Authentication Manager não é exigido para usar o PAM agent.

A versão 8.1 do PAM agent oferece os seguintes benefícios novos:

- Suporte ao Serviço de autenticação da nuvem. O Serviço de autenticação da nuvem usa métodos de autenticação baseados em vários fatores, como Aprovar (notificação por push otimizada para dispositivos móveis), Authenticate Tokencode, Biometria de dispositivo, Tokencode pode SMS, Tokencode por voz e RSA SecurID Tokens, para ajudar no acesso seguro ao SaaS (Software as a Service, software como serviço) e aos aplicativos da Web no local para os usuários.
- Capacidade de acessar o Authentication Manager com o protocolo REST, em vez do protocolo UDP.
- Suporte contínuo ao protocolo UDP usado por versões anteriores do PAM agent.
- O Authentication Manager tem relatórios de agente que ajudam você a gerenciar seus PAM agents instalados com o protocolo REST. No modo REST, o PAM agent pode enviar informações adicionais ao servidor do Authentication Manager, como o número de ID de software exclusivo de cada PAM agent instalado e as informações sobre o sistema operacional usado pelo agente.

Utilizar o PAM agent no modo REST oferece vantagens adicionais em relação ao uso do protocolo UDP:

- Facilita a integração de sua implementação do Authentication Manager com o Serviço de autenticação da nuvem.
- Você pode adicionar e manter um registro de agente de autenticação no Authentication Manager e usá-lo para representar vários agentes instalados.
- Você pode executar vários agentes de autenticação no mesmo hardware com mais facilidade, em comparação ao uso do protocolo UDP.
- Ele usa o protocolo TCP para implementações que exigem que os agentes de autenticação utilizem configurações de rede IPv4 ou o protocolo IPv4.
- Nos modos de autenticação do protocolo REST, a versão 8.1 do PAM agent usa **fips-2.0.16**, o módulo de biblioteca criptográfica compatível com FIPS, com a versão 1.0.2l do OpenSSL. Para obter mais informações, consulte *OpenSSL FIPS 140-2 Security Policy Version 2.0.16* em https://www.openssl.org/docs/fips/SecurityPolicy-2.0.16.pdf.
- Ele exige menos atualizações de agente de autenticação para novos recursos e aprimoramento em comparação aos agentes de autenticação que não usam o protocolo REST. Os agentes de autenticação que usam o protocolo REST têm mais chances de aproveitar as alterações no Authentication Manager, reduzindo assim o número de atualizações necessárias nos vários agentes.

Modos de autenticação

Você pode instalar o PAM agent em um dos três modos de autenticação. Todos os modos fornecem a autenticação do RSA SecurID. Você pode alterar o modo após a instalação, conforme necessário. Para obter

instruções, consulte Alterando o modo de autenticação do PAM Agent Na página 34.

Modo de autenticação	Descrição
RSA Authentication Manager com o protocolo UDP	Autenticadores de hardware e software do RSA SecurID geram tokencodes do RSA SecurID. O agente verifica se os dados digitados pelo usuário correspondem aos dados armazenados no Authentication Manager e permite ou nega o acesso com base no resultado. Por padrão, o upgrade do PAM agent configura o agente para usar o protocolo UDP. Você pode alternar facilmente para um modo de autenticação diferente que utilize o protocolo REST.
RSA Authentication Manager com o protocolo REST	Suporte a todos os tipos de autenticação compatíveis com o Authentication Manager por meio do protocolo REST, como RSA SecurID Tokens e Authenticate Tokencode de software e hardware por meio de uma integração com o componente do Serviço de autenticação da nuvem.
Serviço de autenticação da nuvem com o protocolo REST	Comporta Aprovar (notificação por push otimizada para dispositivos móveis), Authenticate Tokencode, Biometria de dispositivo, Tokencode por SMS, Tokencode por voz e RSA SecurID Tokens. Tokens FIDO e condições de autenticação que requerem combinações de métodos (como Aprovar E RSA SecurID token) não são compatíveis.

O RSA Authentication Agent 8.1 for PAM comporta realms confiáveis do RSA Authentication Manager. O Authentication Manager não aceita RBA (Risk-Based Authentication, autenticação baseada em risco).

Workflow do PAM Agent

O PAM agent é instalado em um servidor UNIX. Ele atua como intermediário entre os usuários da autenticação e o servidor do RSA Authentication Manager ou o Serviço de autenticação da nuvem.

O PAM agent dá suporte aos recursos de segurança do Authentication Manager. Por exemplo, se o Authentication Manager determinar que o usuário associado a um token específico precisa de um novo PIN, o agente solicitará o PIN, que tem as características definidas no Authentication Manager, e enviará as informações ao Authentication Manager. Se o Authentication Manager solicitar o próximo tokencode exibido no token do usuário, o PAM agent alertará o usuário. Se o próximo tokencode correto não for enviado ao Authentication Manager, a autenticação apresentará falha.

Estas etapas descrevem o fluxo de autenticação do PAM agent em todos os três modos de autenticação:

1. Um usuário tenta acessar uma máquina protegida pelo PAM agent, seja localmente, com log-in ou remotamente, com ferramentas como rlogin, telnet, SSH e FTP.

   O usuário deve existir localmente na máquina em que o PAM agent está instalado.

2. A infraestrutura do PAM (Pluggable Authentication Module, módulo de autenticação conectável) do UNIX intercepta todas as solicitações de log-on e usa arquivos de configuração do PAM para acessar o módulo de PAM da RSA:
   - Se um usuário não estiver configurado para a autenticação do RSA SecurID, o módulo de PAM da RSA garantirá o sucesso da solicitação.
   - Se o usuário que solicita acesso é desafiado pelo RSA SecurID, o PAM agent continua a autenticação na etapa 3.

3. Com base no modo de autenticação do PAM agent, o agente contata o Authentication Manager ou o Serviço de autenticação da nuvem.

   Para o Authentication Manager com uma conexão UDP ou o protocolo REST, ocorrem as seguintes etapas:

   a. O agente solicita ao usuário o nome de usuário e, em seguida, o passcode.
   b. O agente envia com segurança o nome de usuário e o passcode ao Authentication Manager:
      - Se o Authentication Manager aprovar a solicitação, o agente concederá acesso ao usuário.
      - Se o Authentication Manager não aprovar a solicitação, o agente negará o acesso.

   Para o Serviço de autenticação da nuvem, ocorrem as seguintes etapas:

   a. O agente solicita ao usuário um nome de usuário e envia as informações ao Serviço de autenticação da nuvem.
   b. O Serviço de autenticação da nuvem apresenta ao agente os métodos de autenticação configurados para o usuário no nível de garantia da política de acesso do Serviço de autenticação da nuvem.
   c. O agente solicita que o usuário seja autenticado.
   d. O usuário escolhe um método de autenticação disponível e é autenticado:
      - Se o Serviço de autenticação da nuvem aprovar a solicitação, o agente concederá acesso ao usuário.
      - Se um método de autenticação não for bem-sucedido, o Serviço de autenticação da nuvem solicitará ao usuário o próximo método de autenticação.
      - Se o Serviço de autenticação da nuvem não aprovar a solicitação, o agente negará o acesso.

Requisitos de software

Esta seção descreve as versões mínimas de software compatíveis com o PAM agent.

Sistema operacional exigido

O PAM agent exige um dos seguintes sistemas operacionais:

- RHEL 6.10: (32 bits e 64 bits)
- RHEL 7.5 (64 bits)
- CentOS Linux 7.5 (64 bits)
- Oracle Linux 6.10 (64 bits)
- Oracle Linux 7.5 (64 bits)

A versão correspondente de 32 bits ou 64 bits do **libuuid.so** (biblioteca UUID) deve ser instalada na máquina do PAM agent.

Requisitos de SELinux

Se o SELinux estiver habilitado em qualquer sistema RHEL ou OracleLinux, você deverá instalar os seguintes pacotes antes de instalar o RSA SecurID Authentication Agent 8.1 for PAM:

selinux-policy-devel*.noarch.rpm
policycoreutils-devel*.rpm

Se o SELinux estiver habilitado no RHEL 6.10 de 32 bits e 64 bits ou no Oracle Linux 6.10 de 64 bits, você deverá instalar os seguintes pacotes antes de instalar o RSA SecurID Authentication Agent 8.1 for PAM:

setools-libs-3.3.7-4.el6.x86_64.rpm
setools-libs-python-3.3.7-4.el6.x86_64.rpm
audit-libs-python-2.4.5-3.el6.x86_64.rpm
libsemanage-python-2.0.43-5.1.el6.x86_64.rpm
policycoreutils-python-2.0.83-29.0.1.el6.x86_64
setroubleshoot-plugins-3.0.40-2.0.1.el6.noarch
setroubleshoot-server-3.0.47-11.0.1.el6.x86_64

Suporte a versões do RSA Authentication Manager

O RSA SecurID Authentication Agent 8.1 for PAM é compatível com a API versão 1.1 do RSA SecurID Authentication, que é a versão atual das APIs REST.

A tabela a seguir lista as versões do RSA Authentication Manager que são necessárias para o suporte a recursos específicos.

Versão exigida do RSA Authentication Manager	Recursos compatíveis
8.2 SP1 ou posterior	O PAM agent exige o RSA Authentication Manager 8.2 SP1 ou posterior.
8.2 SP1 patch 5 ou posterior	Se o indicador de geração de relatórios de agente estiver ativado no PAM agent, o RSA Authentication Manager 8.2 SP1 patch 5 ou posterior será necessário para evitar autenticações com falha no modo REST.
8.3 ou posterior	O RSA Authentication Manager 8.3 e versões posteriores incluem relatórios de agente que ajudam a gerenciar os PAM Agents de protocolo REST instalados. Esses relatórios incluem as informações adicionais que o PAM agent pode enviar ao Authentication Manager.

Suporte a versões do Serviço de autenticação da nuvem

O RSA SecurID Authentication Agent 8.1 for PAM é compatível com a API versão 1.1 do RSA SecurID Authentication, que é a versão atual das APIs REST.

Certificações obrigatórias

O PAM agent usa certificados TLS 1.2 para o protocolo REST. O Serviço de autenticação da nuvem e o RSA Authentication Manager 8.2 ou posterior podem aceitar esses certificados. As implementações que não usam certificados TLS 1.2 devem usar o modo de autenticação que comporta o Authentication Manager com o protocolo UDP.

Nos modos de autenticação do protocolo REST, o PAM agent usa **fips 2.0.16**, o módulo de biblioteca criptográfica compatível com FIPS, com a versão 1.0.2l do OpenSSL. Para obter mais informações, consulte *OpenSSL FIPS 140-2 Security Policy Version 2.0.16* em https://www.openssl.org/docs/fips/SecurityPolicy-2.0.16.pdf.

Ferramentas compatíveis

O PAM agent é compatível com as seguintes ferramentas:

- telnet
- login
- rlogin
- su
- ssh (ssh, sftp e scp)
- sudo

  Faça download e instale a versão sudo compatível de https://www.sudo.ws.

- ftp (limitado a uma transação individual)
- gdm

Suporte a OpenSSH (opcional)

O PAM agent é compatível com OpenSSH 6.0 P1. Se estiver usando OpenSSH, verifique se você está usando a versão compatível do OpenSSH para sua plataforma. O OpenSSH não é obrigatório.

As seguintes ferramentas de OpenSSH são compatíveis:

- ssh
- sftp
- scp

Instale o OpenSSH na máquina do agente. Para saber mais sobre OpenSSH, inclusive os pré-requisitos e o software adicional necessário para compilar o código-fonte, consulte https://www.openssh.com.

Planejando-se para instalar o PAM Agent

Antes de instalar o PAM agent, faça o seguinte:

- Na máquina em que você está instalando o PAM agent:
  1. Obtenha permissões de root.
  2. Crie um diretório **/var/ace** para os arquivos de configuração do PAM agent, caso ele ainda não exista, e crie um diretório de instalação.
  3. Obtenha o certificado CA de raiz confiável do servidor do RSA Authentication Manager ou do Serviço de autenticação da nuvem. (Para obter instruções, consulte o artigo Como exportar o RSA SecurID Access Authentication Manager ou Certificado raiz do serviço de autenticação em nuvem da base de conhecimento.) Depois, faça o seguinte:
     a. Verifique se o certificado não expirou.
     b. Armazene o certificado no formato PEM. Se houver vários certificados CA, eles precisarão ser concatenados em um único arquivo no formato PEM.
     c. Copie ***filename*.pem** no diretório **/var/ace/**.
     d. Proteja o diretório **/var/ace/** que contém os certificados com os privilégios adequados.

- Para fazer a autenticação com o RSA Authentication Manager, crie um registro de agente de autenticação para o PAM agent no banco de dados interno. Para obter mais informações, entre em contato com o Super Admin do Authentication Manager ou consulte a Ajuda do Authentication Manager na RSA Link.
- Para fazer a autenticação com o protocolo UDP, você deve gerar o arquivo de configuração do Authentication Manager, **sdconf.rec**, ou obter este arquivo com o Super Admin do Authentication Manager. Esse arquivo não é necessário para a autenticação com o protocolo REST.

  O arquivo **sdconf.rec** especifica como o agente se comunica com a instância primária e as instâncias de réplica do Authentication Manager por endereço IP. Faça o seguinte:

  - Certifique-se de que a versão mais recente do arquivo **sdconf.rec** esteja em um diretório acessível na máquina do agente, como o diretório padrão **/var/ace**.
  - Você deve ter permissão de gravação no diretório onde o arquivo **sdconf.rec** está armazenado.
- No modo de autenticação que usa o Serviço de autenticação da nuvem com o protocolo REST, o PAM agent depende do Serviço de autenticação da nuvem para o balanceamento de carga e o failover.
- No modo de autenticação que usa o RSA Authentication Manager com o protocolo REST, o PAM agent não comporta o balanceamento de carga. O PAM agent comporta o failover de até 15 instâncias de réplica do Authentication Manager.
- Colete as informações que você especificará durante a instalação do PAM agent.

  Authentication Manager com o protocolo UDP. Você pode manter os valores padrão ou especificar novos diretórios.

Descrição	**Seu plano**
Diretório onde **sdconf.rec** está localizado. O valor padrão é **/var/ace/**.	
Caminho da raiz para o diretório do PAM agent. O valor padrão é **/opt**.	

  Authentication Manager com o protocolo REST. Solicite ao Super Admin do Authentication Manager as seguintes informações:

Descrição	**Seu plano**
URL do servidor REST para a comunicação entre o agente de autenticação e a instância primária do Authentication Manager. Use o seguinte formato: `https://`*`HOSTNAME`*`:`*`PORT_NO`*`/mfa/v1_1/authn` Na instância primária, obtenha o valor de *`HOSTNAME`* do campo **Nome do domínio completo** na página **Administração > Rede > Configurações de rede do dispositivo** do Console de operações. A *`PORTA`* padrão é 5555.	
Número de instâncias de réplica do	

Descrição	Seu plano
Authentication Manager que podem ser usadas para failover.	
URL do servidor REST de cada instância de réplica. Use o seguinte formato: `https://HOSTNAME:PORT_NO/mfa/v1_1/authn` Na instância de réplica, obtenha o valor de *HOSTNAME* do campo **Nome do domínio completo** na página **Administração > Rede > Configurações de rede do dispositivo** do Console de operações. A *PORTA* padrão é 5555.	
A chave de acesso (chave do client) para aprovar com segurança as solicitações de autenticação de usuário para o Authentication Manager. Esse valor é gerado no Console de segurança na instância primária do Authentication Manager. Para instruções sobre como obter a chave de acesso, consulte o tópico a seguir no link da RSA: Configurar a API do RSA SecurID Authentication para agentes de autenticação.	
Informe o diretório e o nome do arquivo para o certificado confiável do servidor no agente de autenticação. O valor padrão é **/var/ace/cert.pem**.	
Nome do agente de autenticação (ID do client) que foi criado para o PAM agent no Authentication Manager.	
Caminho da raiz para o diretório do PAM agent. O valor padrão é **/opt**.	

Serviço de autenticação da nuvem com o protocolo REST. Solicite ao Super Admin do Serviço de autenticação da nuvem as seguintes informações:

Descrição	Seu plano
URL do servidor REST para a comunicação entre o agente e o Serviço de autenticação da nuvem. Use o seguinte formato: `https://HOSTNAME:PORT/mfa/v1_1/authn` Para o Serviço de autenticação da nuvem, obtenha o valor de *HOSTNAME* do campo	

Descrição	Seu plano
Domínio do serviço de autenticação na guia **Registro** da página de configurações de qualquer roteador de identidade no Cloud Administration Console. A *PORTA* padrão é 443.	
Chave da API de autenticação (chave do client) criada no Cloud Administration Console para aprovar com segurança as solicitações de autenticação de usuário no Serviço de autenticação da nuvem. Para instruções sobre como obter a chave da API de autenticação, consulte o tópico a seguir no link da RSA: Adicionar uma chave de API do RSA SecurID Authentication.	
Diretório e nome do arquivo para o certificado confiável do servidor no agente de autenticação. O valor padrão é **/var/ace/cert.pem**.	
ID do tenant do Serviço de autenticação da nuvem. O PAM agent pode fornecer o ID do tenant em solicitações de autenticação, mas o agente não valida os dados. Atualmente, não há suporte para este parâmetro no Serviço de autenticação da nuvem.	
Nome da política de acesso do Serviço de autenticação da nuvem. Essa política é definida no Cloud Administration Console.	
Nome do agente de autenticação CLIENT_ID a ser exibido nas notificações móveis. Você pode informar qualquer valor. Por exemplo, PAM_Agent.	
Caminho da raiz para o diretório do PAM agent. O valor padrão é **/opt**.	

Instalando o RSA Authentication Agent 8.1 for PAM

Conclua as seguintes tarefas para instalar o PAM agent:

1. Especificar o endereço IP do agente para o modo UDP Na página seguinte
2. Configurar o OpenSSH Na página seguinte
3. Instalar o PAM Agent Na página 19
4. Para o modo UDP, faça um teste de autenticação. Para obter mais informações, consulte Utilitários de autenticação para o modo UDP Na página 41.

   Para o modo de protocolo REST, teste a conexão acessando a URL do servidor REST por meio de qualquer

navegador ou client http. Por exemplo, digite https://*HOSTNAME*:*PORT_NO*/mfa/v1_1/authn. Como você não está fazendo uma autenticação no momento, seu navegador ou client http deverá exibir uma resposta de HTTP "Proibido" ou "Não autorizado".

5. Habilitar o SELinux Na página 22 (se necessário).

Especificar o endereço IP do agente para o modo UDP

Para o modo UDP, você deve criar o arquivo **sdopts.rec** no mesmo diretório usado pelo arquivo **sdconf.rec**. Este procedimento não se aplica ao modo REST.

Arquivo	Descrição
sdopts.rec	Lista o endereço IP da máquina na qual o agente está instalado. O agente usa o endereço IP do arquivo **sdopts.rec** para se comunicar com o RSA Authentication Manager.
sdconf.rec	Especifica os endereços IP que são usados pelo Authentication Manager.

Procedimento

1. Na máquina do agente, use um editor de texto para criar um arquivo **sdopts.rec** no caminho onde o arquivo **sdconf.rec** está salvo.
2. No arquivo, digite:

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

   onde *x.x.x.x* é o endereço IP do host do agente.

   Obs.: Use somente letras maiúsculas e não inclua espaços.

3. Salve o arquivo.

Configurar o OpenSSH

Se estiver usando OpenSSH, a suíte de utilitários de rede relacionados à segurança com base no SSH (Secure Shell Protocol), você deverá configurar esse software para funcionar com o PAM agent e para exibir mensagens de autenticação com passcode aos usuários.

Antes de começar

Instale o OpenSSH na máquina do agente. Para saber mais sobre OpenSSH, inclusive os pré-requisitos e o software adicional necessário para compilar o código-fonte, consulte https://www.openssh.com.

Procedimento

1. Na máquina do agente, abra o arquivo **sshd_config**.
2. Defina os seguintes parâmetros e salve as alterações:

Parâmetro	Configuração
UsePAM	sim
PasswordAuthentication	no
ChallengeResponseAuthentication	sim

   Definir o parâmetro PasswordAuthentication como no desabilita o prompt de senha do OpenSSH. Em vez disso, o PAM agent é usado. Como resultado, o usuário é solicitado apenas a fazer a autenticação do SecurID.

3. Reinicie o sshd. Digite:

   ```
   service sshd restart
   ```

Instalar o PAM Agent

Você pode instalar manualmente o PAM agent em máquinas individuais ou pode escolher uma instalação silenciosa para automatizar o processo de implementação de várias cópias do PAM agent.

Instalar o PAM Agent em uma máquina

Execute esta tarefa para instalar um PAM agent. Para instalar o PAM agent em mais de uma máquina, consulte Instalação em massa do PAM Agent com a instalação silenciosa Na página seguinte.

Procedimento

1. Na máquina do agente, altere para o diretório do programa de instalação do PAM agent.
2. Descompacte o arquivo digitando:

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

3. Execute o script de instalação digitando:

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

4. Siga as solicitações. Pressione ENTER para aceitar o valor padrão ou informe o valor apropriado.

   Para o modo UDP do RSA Authentication Manager, faça o seguinte:

   - Aceite a licença do software da RSA.
   - Digite 0 para selecionar o RSA Authentication Manager com o modo de autenticação do protocolo UDP.
   - Informe o diretório onde **sdconf.rec** está localizado.
   - Informe o diretório de instalação do PAM agent.

   Para o modo REST do RSA Authentication Manager, faça o seguinte:

   - Aceite a licença do software da RSA.
   - Digite 1 para selecionar o RSA Authentication Manager com o modo de autenticação do protocolo REST.
   - Digite a URL do servidor REST para a comunicação entre o agente de autenticação e a instância primária.
   - Digite y se houver instâncias de réplica do Authentication Manager para failover.
   - Especifique o número de instâncias de réplica.
   - Digite a URL do servidor REST para cada instância de réplica.
   - Digite a chave do client (chave de acesso) a fim de aprovar com segurança as solicitações de autenticação para o Authentication Manager.
   - Informe o diretório e o nome do arquivo para o certificado confiável do servidor no agente de autenticação.
   - Digite o ID do cliente, que é o nome do agente de autenticação no Authentication Manager.
   - Informe o diretório de instalação do PAM agent.

Para o modo REST do Serviço de autenticação da nuvem, faça o seguinte:

- Aceite a licença do software da RSA.
- Digite 2 para selecionar o Serviço de autenticação da nuvem com o modo de autenticação do protocolo REST.
- Digite a URL do servidor REST para a comunicação entre o agente de autenticação e o Serviço de autenticação da nuvem.
- Digite a chave do client (chave da API de autenticação) a fim de aprovar com segurança as solicitações de autenticação para o Serviço de autenticação da nuvem.
- Informe o diretório e o nome do arquivo para o certificado confiável do servidor no agente de autenticação.
- Digite o ID do tenant para o Serviço de autenticação da nuvem.
- Especifique o nome da política de acesso do Serviço de autenticação da nuvem.
- Digite o nome do agente de autenticação CLIENT_ID a ser exibido nas notificações móveis.
- Informe o diretório de instalação do PAM agent.

5. Somente para o modo UDP, verifique se VAR_ACE no arquivo **/etc/sd_pam.conf** indica o local correto do arquivo **sdconf.rec**. Esse é o caminho para os arquivos de configuração. O caminho inteiro deve ter a permissão de root -rw-------.

Depois de concluir

- Você pode verificar a instalação conferindo o arquivo **installer.log** no diretório do programa de instalação do PAM agent.
- Para o modo UDP, faça um teste de autenticação. Para obter mais informações, consulte Utilitários de autenticação para o modo UDP Na página 41.
- Para o modo de protocolo REST, teste a conexão acessando a URL do servidor REST por meio de qualquer navegador ou client http. Por exemplo, digite https://*HOSTNAME*:*PORT_NO*/mfa/v1_1/authn. Como você não está fazendo uma autenticação no momento, seu navegador ou client http deverá exibir uma resposta de HTTP "Proibido" ou "Não autorizado".

Instalação em massa do PAM Agent com a instalação silenciosa

Execute esta tarefa para implementar um grande número de PAM agents com informações sobre configuração idênticas. Por exemplo, execute esta tarefa se precisar instalar um grande número de agentes que se comuniquem com os mesmos servidores do RSA Authentication Manager ou o mesmo Serviço de autenticação da nuvem.

Antes de começar

Instale manualmente o PAM agent e registre os prompts. Para obter instruções, consulte Instalar o PAM Agent em uma máquina Na página anterior.

Procedimento

1. Crie um arquivo de configuração com base em texto, no qual você especificará opções de configuração do script de instalação do PAM agent. Você pode escolher qualquer nome para o arquivo de configuração, tal como **installoptions.conf**.
2. Abra o arquivo e liste em uma linha separada cada opção de configuração que você deseja selecionar, na mesma ordem em que os prompts são apresentados durante uma instalação manual do PAM agent.

O exemplo a seguir descreve o prompt correspondente para cada opção especificada na configuração do UDP:

Valor de exemplo	Opção
y	Continuar instalação silenciosa? (s) Este prompt sempre é incluído primeiro.
Accept	Aceitar os termos e condições da licença? (Aceitar)
0	Modo de autenticação? (valor numérico para o modo desejado) 0: RSA Authentication Manager com o protocolo UDP 1: RSA Authentication Manager com o protocolo REST 2: Serviço de autenticação em nuvem com o protocolo REST
/var/ace	O diretório contém sdconf.rec? (caminho do diretório)
/opt	Caminho de instalação para o diretório do PAM agent? (caminho do diretório)
y	Fazer upgrade/sobregravar a instalação existente? (s/n)

Nesse caso, o arquivo de configuração com base em texto deve conter:

```
y
Accept
0
/var/ace
/opt
y
```

Como outro exemplo, para o modo REST do Authentication Manager, o arquivo de configuração pode conter dados semelhantes ao seguinte:

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

Obs.: o número e a ordem dos prompts de instalação variam de acordo com o modo e plataforma do PAM agent que você está instalando.

3. Altere para o diretório de instalação do PAM agent.
4. Descompacte o arquivo digitando:

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

5. Execute o script de instalação digitando:

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

   onde ***installoptions.conf*** é o arquivo de configuração que você criou na Etapa 1. Se o arquivo de configuração estiver em um local diferente do diretório atual, especifique o caminho completo para o arquivo ***installoptions.conf***.

Habilitar o SELinux

Depois de instalar o PAM agent, você pode habilitar o SELinux (Security-Enhanced Linux).

Antes de começar

- Na máquina do agente, verifique se o PAM agent está funcionando.

  Por exemplo, no modo UDP, faça uma autenticação de teste ou, no modo REST, tente fazer ping em um servidor do Authentication Manager ou no Serviço de autenticação da nuvem. Para obter mais informações sobre o modo UDP de teste, consulte Utilitários de autenticação para o modo UDP Na página 41.

- Crie um backup dos diretórios **/etc/sd_pam.conf** e **/var/ace**.
- Para evitar o bloqueio do acesso à máquina do PAM agent, configure as ferramentas protegidas do RSA SecurID para que usem o módulo de PAM padrão fornecido com seu sistema operacional, e não o módulo de PAM da RSA. Reverta a configuração da ferramenta para funcionar sem o RSA Authentication Agent 8.1 for PAM.

  Feche todas as sessões ativas usando os módulos de PAM da RSA.

  Obs.: se desinstalar o módulo da RSA enquanto houver referências ao módulo da RSA no diretório **/etc/pam.d**, você ficará bloqueado fora de seu sistema.

Procedimento

1. Na máquina do agente, habilite o SELinux.
2. Reinstale o PAM agent a fim de criar políticas do SELinux para todas as ferramentas:
   a. Execute o script de instalação digitando:

      /<filename>/install_pam.sh

   b. Digite **y** quando o programa de instalação perguntar se você deseja sobregravar a instalação atual.
   c. Substitua a política do SELinux existente. Quando solicitado, digite **y** ou pressione ENTER para selecionar o valor padrão **yes**.

Depois de concluir

- Habilite `auth required pam_securid.so` para qualquer ferramenta configurada e teste a autenticação.
- Se o SELinux estiver habilitado e se o arquivo **cert.pem** estiver instalado em um diretório personalizado, em vez do diretório padrão **/var/ace/**, você deverá habilitar a política do SELinux no diretório personalizado.

  Execute os seguintes comandos, onde *cust_cert* é o diretório de certificados personalizado:

```
semanage fcontext -a -t var_t '/cust_cert/cert.pem'

restorecon -v '/cust_cert/cert.pem'
```

Upgrade para o RSA Authentication Agent 8.1 for PAM

Você pode fazer upgrade para o RSA Authentication Agent 8.1 for PAM a partir da versão 7.1 Patch 2 (7.1.0.2) ou da versão 8.0.

Ao fazer upgrade da versão 7.1.0.2, um agente que recebeu upgrade usa o RSA Authentication Manager e o protocolo UDP para a autenticação. Você pode alterar o modo de autenticação para utilizar o Serviço de autenticação da nuvem ou o Authentication Manager e o protocolo REST. Para obter instruções, consulte Alterando o modo de autenticação do PAM Agent Na página 34.

Ao fazer upgrade da versão 8.0, o agente que recebeu upgrade mantém o mesmo modo de autenticação que foi configurado para a versão anterior.

Antes de começar

- Você deve ter permissões de root no host do agente e permissão de gravação no diretório no qual o arquivo **sdconf.rec** está armazenado. Esse arquivo é normalmente armazenado no diretório padrão **/var/ace**.
- Faça backup dos arquivos de configuração antes da sobregravação para salvar as definições de configuração. Para obter mais informações, consulte Arquivos de configuração essenciais Na página 52.
- Configure as ferramentas protegidas do RSA SecurID para que usem o módulo de PAM padrão fornecido com seu sistema operacional, e não o módulo de PAM da RSA. Todas as sessões ativas usando os módulos de PAM da RSA deverão ser fechadas antes de você continuar com o upgrade.

Procedimento

1. Na máquina do agente, altere para o diretório do programa de instalação do PAM agent.
2. Descompacte o arquivo digitando:

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

3. Execute o script de instalação digitando:

   ```
   /<filename>/install_pam.sh
   ```

4. Sobregrave os arquivos de instalação existentes. Digite **y** quando o programa de instalação perguntar se você deseja sobregravar a instalação atual.
5. Se o SELinux estiver habilitado e você planejar usar o protocolo REST para a autenticação, você deverá sobregravar a política do SELinux existente. Quando solicitado, digite **y** ou pressione ENTER para selecionar o valor padrão **yes**.

   Se você digitar **n**, algumas ferramentas não poderão ser autenticadas com o protocolo REST. No entanto, você pode sobregravar a política do SELinux existente executando o script de instalação novamente. Os arquivos que já receberam upgrade não serão afetados.

6. Obtenha o número da versão do agente para determinar se o upgrade foi bem-sucedido. Digite:

   strings pam_securid.so | grep "Agent"

Isso retorna o número da versão do agente instalado.

Configurando ferramentas

Você deve configurar as ferramentas compatíveis para alertar os usuários com os métodos de autenticação compatíveis com o Serviço de autenticação da nuvem e o RSA Authentication Manager.

Obs.: o número de configurações de usuário simultâneas permitidas no servidor Unix deve ser definido para cada ferramenta, para o sistema operacional utilizado e para os log-ons simultâneos esperados no servidor, principalmente ao usar o Serviço de autenticação da nuvem. Por exemplo, defina a configuração "MaxStartups" no arquivo **/etc/ssh/sshd_config** como SSH e a configuração "Instances" no arquivo **/etc/xinetd.d/telnet** como telnet.

Configurar telnet abaixo

Configurar login abaixo

Configurar rlogin Na página oposta

Configurar su Na página oposta

Configurar ssh e ferramentas relacionadas Na página oposta

Configurar sudo Na página oposta

Configurar ftp Na página 26

Configurar gdm Na página 26

Configurar telnet

Configure telnet para solicitar aos usuários os métodos de autenticação compatíveis com o Serviço de autenticação da nuvem e o RSA Authentication Manager.

Procedimento

Obs.: o PAM agent 8.1 não aceita telnet de kerberos.

1. Altere para o diretório **/etc/pam.d**.
2. Abra o arquivo **remote**.
3. Comente quaisquer linhas que comecem com `auth`.
4. Adicione a linha:

   ```
   auth required pam_securid.so
   ```

5. Apenas para Oracle Linux 6.8 (64 bits), repita essas etapas para o arquivo **/etc/pam.d/login**.

   Para todas as outras versões do RHEL e Oracle Linux, o procedimento está concluído.

Configurar login

Configure o comando login para solicitar aos usuários os métodos de autenticação compatíveis com o Serviço de autenticação da nuvem e o RSA Authentication Manager.

1. Altere para o diretório **/etc/pam.d**.
2. Abra o arquivo **login**.

3. Comente as linhas que começam com `auth`.
4. Adicione a linha:

```
auth required pam_securid.so
```

Configurar rlogin

Configure o utilitário rlogin para solicitar aos usuários os métodos de autenticação compatíveis com o Serviço de autenticação da nuvem e o RSA Authentication Manager.

Antes de começar

Se o rlogin não estiver funcionando no RHEL 6.8 ou Oracle Linux 6.8, siga os procedimentos de Problemas de configuração conhecidos Na página 40.

Procedimento

1. Altere para o diretório **/etc/pam.d**.
2. Abra o arquivo **rlogin**.
3. Comente as linhas que começam com `auth`.
4. Adicione a linha:

```
auth required pam_securid.so
```

Configurar su

Configure o comando su para solicitar aos usuários os métodos de autenticação compatíveis com o Serviço de autenticação da nuvem e o RSA Authentication Manager.

Procedimento

1. Altere para o diretório **/etc/pam.d**.
2. Abra o arquivo **su**.
3. Comente quaisquer linhas que comecem com `auth`.
4. Adicione a linha:

```
auth required pam_securid.so
```

Configurar ssh e ferramentas relacionadas

Você pode configurar o SSH e as ferramentas relacionadas, como scp e sftp, para solicitar aos usuários os métodos de autenticação compatíveis com o Serviço de autenticação da nuvem e o RSA Authentication Manager.

Procedimento

1. Altere para o diretório **/etc/pam.d**.
2. Abra o arquivo **sshd**.
3. Comente as linhas que começam com `auth`.
4. Adicione a linha:

```
auth required pam_securid.so
```

Configurar sudo

Se precisar de sudo, você deverá configurar o comando sudo para solicitar aos usuários os métodos de

autenticação compatíveis com o Serviço de autenticação da nuvem e o RSA Authentication Manager.

Antes de começar

Faça download e instale a versão sudo compatível de https://www.sudo.ws.

Procedimento

1. Altere para o diretório **/etc/pam.d**.
2. Abra o arquivo **sudo**.
3. Comente quaisquer linhas que comecem com `auth`.
4. Adicione a linha:

```
auth required pam_securid.so
```

Configurar ftp

Configure o protocolo ftp para solicitar aos usuários os métodos de autenticação compatíveis com o RSA Authentication Manager.

Não é possível usar o Serviço de autenticação da nuvem para proteger o ftp. No entanto, você pode usar sftp. Para obter instruções, consulte Configurar ssh e ferramentas relacionadas Na página anterior.

Procedimento

1. Altere para o diretório **/etc/pam.d**.
2. Abra o arquivo **vsftpd**.
3. Comente as linhas que começam com `auth`.
4. Adicione a linha:

```
auth required pam_securid.so
```

Configurar gdm

Você pode configurar gdm para solicitar aos usuários os métodos de autenticação compatíveis com Serviço de autenticação da nuvem e RSA Authentication Manager.

Procedimento

1. Altere para o diretório **/etc/pam.d**.
2. Modifique os arquivos **gdm**, **gdm-password** e **gdm-autologin** da seguinte maneira:
    a. Abra cada arquivo gdm.
    b. Comente quaisquer linhas que comecem com `auth`.
    c. Adicione a linha:

```
auth required pam_securid.so
```

Capítulo 2: Configurando recursos

Configurando recursos do agente e do Unix

Você pode personalizar a configuração do PAM agent para usar o agente opcional e os recursos do UNIX.

Obs.: antes de personalizar o agente, faça cópias de backup dos arquivos de configuração originais.

Vários arquivos de configuração estão localizados no diretório **/etc/pam.d**. Cada arquivo usa o nome da ferramenta de conexão.

Para personalizar o agente, consulte:

Habilitar a geração de relatórios do agente para o RSA SecurID Authentication Agent 8.1 for PAM abaixo

Habilitar a saída de depuração abaixo

Habilitar o registro de rastreamento do SecurID para o modo UDP Na página oposta

Configurar módulos agrupáveis Na página oposta

Usar senhas de reserva Na página 30

Habilitar a autenticação seletiva do SecurID Na página 31

Configurar o tempo de retirada exponencial Na página 32

Habilitar a geração de relatórios do agente para o RSA SecurID Authentication Agent 8.1 for PAM

Você pode configurar o parâmetro ENABLE_AGENT_REPORTING no arquivo **mfa_api.properties** a fim de enviar detalhes do agente, como o nome de host, a versão do agente e a versão de SO, para o RSA Authentication Manager. Você pode usar o RSA Authentication Manager 8.3 ou posterior para executar relatórios que contenham esses detalhes.

Antes de começar

Você deve ter permissões de root na máquina em que o agente está instalado e permissão de gravação no diretório onde o arquivo **mfa_api.properties** está armazenado. Por padrão, esse arquivo é armazenado em **/var/ace/conf**.

Procedimento

1. Altere para o diretório onde **mfa_api.properties** está localizado. Por padrão, o diretório é **/var/ace/conf**.
2. Abra **mfa_api.properties**.
3. Altere o parâmetro ENABLE_AGENT_REPORTING para 1, o que habilita a geração de relatórios do agente. O valor padrão é 0.
4. Salve o arquivo.

   Informações sobre o PAM agent e a máquina onde ele está instalado estão incluídas nos detalhes de geração de relatórios do PAM agent que são enviados ao Authentication Manager.

Habilitar a saída de depuração

Para a solução de problemas, você pode habilitar a saída de depuração de ferramentas específicas que são usadas pelo PAM agent.

Você também pode configurar o log do sistema para gravar todas as mensagens de log de autenticação do PAM agent. Para obter mais informações, consulte Registro do PAM Agent Na página 45.

Procedimento

1. Altere para o diretório **/etc/** e abra o arquivo **pam.d**.
2. Edite o arquivo apropriado adicionando um argumento de depuração ao módulo pam_securid.so. Digite:

   ```
   auth required pam_securid.so debug
   ```

Habilitar o registro de rastreamento do SecurID para o modo UDP

Você pode habilitar o registro detalhado de rastreamento do SecurID para o PAM agent e para os utilitários de autenticação acetest e acestatus. Por padrão, quando você instala o PAM agent, o registro de rastreamento do SecurID está desabilitado.

Procedimento

1. Altere para o diretório **/etc/** e abra o arquivo **sd_pam.conf**.
2. Para habilitar o registro detalhado do agente e definir o nível de registro, configure a seguinte variável:

   `RSATRACELEVEL=`*`value`*

   Onde *value* é uma configuração da tabela a seguir.

Valor	Descrição
0	Desabilita o registro (padrão)
1	Registra mensagens regulares
2	Registra pontos iniciais de função
4	Registra pontos finais de função
8	Todos os controles de fluxo lógico usam isto (ifs)

   Para combinações, adicione os valores correspondentes. Por exemplo, para registrar mensagens regulares e pontos iniciais de função, defina o valor 3.

3. Especifique o caminho do arquivo para onde os registros serão redirecionados. Defina a seguinte variável:

   `RSATRACEDEST=`*`filepath`*

   Onde *filepath* é o caminho do arquivo.

   Por padrão, essa variável está em branco. Se você não definir essa variável, os registros vão gerar um erro padrão para os utilitários de autenticação acetest e acestatus, e nenhum registro será gerado para as ferramentas de autenticação, mesmo quando o valor `RSATRACELEVEL` for especificado.

4. Salve suas alterações.

Configurar módulos agrupáveis

Em uma configuração agrupada, você pode usar o agente para integrar o módulo de autenticação de PAM do RSA SecurID a outros módulos de autenticação de PAM em seu ambiente. A senha ou passcode é transmitido de um módulo de autenticação ao próximo. Você pode configurar a prioridade dos desafios de autenticação ao editar o arquivo de configuração **/etc/pam.d/*tool name*** adequado.

Obs.: os argumentos use_first_pass e try_first_pass não são aceitos quando uma configuração agrupada é usada com o Serviço de autenticação da nuvem.

O agente trabalha com estes argumentos:

- **use_first_pass.** O agente usa apenas a senha ou passcode transmitido a partir do módulo anterior e nega o acesso se as credenciais não correspondem. O usuário não é solicitado a se autenticar novamente.
- **try_first_pass.** O agente usa a senha ou passcode transmitido a partir do módulo anterior. Se as credenciais não corresponderem, o usuário será solicitado a se autenticar.
- **not_set_pass.** O agente não envia a senha ou o passcode para o módulo de senha agrupado.

Obs.: quando os usuários excluídos da autenticação do SecurID fazem tentativas de log-in com falha para acessar o módulo de PAM da RSA, o recurso de retirada exponencial garante que o módulo de PAM da RSA retenha o controle até que o log-in seja bem-sucedido ou a sessão de autenticação seja encerrada. Para obter mais informações sobre a configuração do tempo de retirada exponencial, consulte Configurar o tempo de retirada exponencial Na página 32.

A seção a seguir apresenta um exemplo de como configurar uma ferramenta de conexão (ferramenta de log-in) em um ambiente agrupado.

Procedimento

1. Altere para **/etc/pam.d** e abra o arquivo **login**.

   O seguinte texto será exibido:

   ```
   #%PAM-1.0
   auth required pam_securetty.so
   auth required pam_stack.so service=system-auth
   auth required pam_nologin.so
   account required pam_stack.so service=system-auth
   password required pam_stack.so service=system-auth
   # pam_selinux.so close should be the first session rule
   session required pam_selinux.so close
   session required pam_stack.so service=system-auth
   session required pam_loginuid.so
   session optional pam_console.so
   # pam_selinux.so open should be the last session rule
   session required pam_selinux.so open
   ```

2. Comente as seguintes linhas:

   ```
   auth required pam_securetty.so
   auth required pam_stack.so service=system-auth
   auth required pam_nologin.so
   ```

3. Adicione as linhas a seguir. Digite:

   ```
   auth required pam_securid.so
   ```

Usar senhas de reserva

O recurso de senha de reserva é um método de acesso de emergência que permite que você, o administrador, faça a autenticação na máquina protegida em que o agente está instalado sem digitar um passcode do RSA SecurID. O PAM agent permite que apenas os administradores root usem senhas de reserva durante

circunstâncias imprevistas, como a perda de comunicação entre o agente e o RSA SecurID Authentication Agent 8.1 for PAM. Nessas situações, os administradores podem desabilitar temporariamente o agente, caso os usuários precisem de acesso imediato aos recursos hospedados.

Obs.: a senha do UNIX é a senha de reserva.

Procedimento

1. Abra o arquivo apropriado em **/etc/pam.d.**
2. Adicione um argumento de reserva ao módulo pam_securid.so. Digite:

```
auth required pam_securid.so reserve
```

Habilitar a autenticação seletiva do SecurID

Você pode configurar o agente para sempre ou nunca solicitar, de modo seletivo, que usuários ou grupos específicos do UNIX sejam autenticados no SecurID:

Habilitar a autenticação seletiva do SecurID para grupos do UNIX abaixo

Habilitar a autenticação seletiva do SecurID para usuários do UNIX Na página seguinte

Obs.: quando as duas opções de suporte seletivo – para grupos e usuários – estão habilitadas, apenas o suporte seletivo a usuários fica habilitado, e o suporte seletivo a grupos é ignorado.

A tabela a seguir lista os possíveis valores que podem ser definidos no arquivo **sd_pam.conf**.

ENABLE_ GROUPS_ SUPPORT	ENABLE_ USERS_ SUPPORT	Resultado
0	0	Nenhum recurso é ativado. Todos os usuários e grupos de usuários são desafiados.
0	1	O suporte ao usuário selecionado está habilitado. O PAM agent sempre solicita que usuários específicos do UNIX sejam autenticados com o SecurID ou nunca solicita que usuários específicos sejam autenticados com o SecurID.
1	0	O suporte ao grupo selecionado está habilitado. O PAM agent sempre solicita que grupos específicos do UNIX sejam autenticados com o RSA SecurID ou nunca solicita que grupos específicos sejam autenticados com o SecurID.
1	1	O suporte ao usuário selecionado está habilitado. O PAM agent sempre solicita que usuários específicos do UNIX sejam autenticados com o SecurID ou nunca solicita que usuários específicos sejam autenticados com o SecurID.

Habilitar a autenticação seletiva do SecurID para grupos do UNIX

Você pode configurar o PAM agent para sempre ou nunca solicitar que grupos específicos do UNIX sejam autenticados com o RSA SecurID. Quando o PAM agent é instalado, esse recurso não é habilitado.

Os membros do grupo excluídos da autenticação do SecurID podem ser autenticados com credenciais do UNIX ou por meio de outro módulo de PAM na pilha. Para isso, configure o parâmetro PAM_IGNORE_SUPPORT.

Obs.: Não especifique grupos do RSA Authentication Manager. Esse recurso se destina apenas aos grupos do UNIX.

Procedimento

1. Altere para o diretório **/etc** e abra o arquivo **sd_pam.conf**.
2. Defina o parâmetro ENABLE_GROUP_SUPPORT como 1. O valor padrão é 0.
3. Preencha o parâmetro LIST_OF_GROUPS.
4. Defina o valor do parâmetro INCL_EXCL_GROUPS.
   Os valores válidos são:
   0 – Desabilitar a autenticação do SecurID para os grupos listados (padrão).
   1 – Habilitar a autenticação do SecurID somente para os grupos listados.
5. (Opcional) Defina o parâmetro PAM_IGNORE_SUPPORT.
   Os valores válidos são:
   0 – Habilitar a autenticação por senha do UNIX (padrão).
   1 – Desabilitar a autenticação por senha do UNIX.
   Este parâmetro se aplica somente aos grupos excluídos da autenticação do SecurID.
6. Salve o arquivo.

Habilitar a autenticação seletiva do SecurID para usuários do UNIX

Você pode configurar o PAM agent para sempre ou nunca solicitar que usuários específicos do UNIX sejam autenticados com o SecurID. Quando o PAM agent é instalado, esse recurso não é habilitado.

Os usuários excluídos da autenticação do SecurID podem ser autenticados com credenciais do UNIX ou por meio de outro módulo de PAM na pilha. Para isso, configure o parâmetro PAM_IGNORE_SUPPORT_FOR_USERS.

Procedimento

1. Altere para o diretório **/etc** e abra o arquivo **sd_pam.conf**.
2. Defina o parâmetro ENABLE_USERS_SUPPORT como 1. O valor padrão é 0.
3. Preencha o parâmetro LIST_OF_USERS.
4. Defina o valor do parâmetro INCL_EXCL_USERS.
   Os valores válidos são:
   0 – Desabilitar a autenticação do SecurID para os usuários listados (padrão).
   1 – Habilitar a autenticação do SecurID somente para os usuários listados.
5. (Opcional) Defina o parâmetro PAM_IGNORE_SUPPORT_FOR_USERS.
   Os valores válidos são:
   0 – Habilitar a autenticação por senha do UNIX (padrão).
   1 – Desabilitar a autenticação por senha do UNIX.
   Este parâmetro se aplica somente aos usuários excluídos da autenticação do SecurID.
6. Salve o arquivo.

Configurar o tempo de retirada exponencial

Você pode configurar o tempo que um usuário que está excluído da autenticação do RSA SecurID deverá aguardar antes da autenticação após cada tentativa sucessiva de log-in com falha. Por padrão, os usuários podem repetir a autenticação do UNIX depois de uma tentativa de log-in com falha com um atraso de pow(4, failattempts) segundos. Por exemplo, 3 tentativas de login com falha resultam em um atraso de 64 segundos (4 à potência de 3 ou 4 x 4 x 4 = 64).

Obs.: o protocolo ftp não comporta o atraso de retirada exponencial.

Procedimento

1. Altere para o diretório **/etc** e abra o arquivo **sd_pam.conf**.
2. Defina o parâmetro BACKOFF_TIME_FOR_RSA_EXCLUDED_UNIX_USERS como *N*, da seguinte maneira:

N	**Comportamento da autenticação**
0	Desativar a autenticação repetida do UNIX após uma tentativa de log-in com falha. Não há atraso de autenticação para as tentativas de log-in após uma tentativa de login com falha.
1,2,3	Habilitar a repetição da autenticação do UNIX depois de uma tentativa de log-in com falha com um atraso de pow(3, failattempts) segundos.
4	Habilitar a repetição da autenticação do UNIX depois de uma tentativa de log-in com falha com um atraso de pow(4, failattempts) segundos.
5/Acima	Habilitar a repetição da autenticação do UNIX depois de uma tentativa de log-in com falha com um atraso de pow(5/Above, failattempts) segundos.

Substituir o certificado da CA de raiz confiável do servidor

Talvez seja necessário substituir o certificado da CA de raiz confiável do servidor, por exemplo, se o certificado RSA Authentication Manager ou Serviço de autenticação da nuvem atual for atualizado.

Para instruções sobre obtenção do certificado, consulte o artigo Como exportar o RSA SecurID Access Authentication Manager ou Certificado raiz do serviço de autenticação em nuvem da base de conhecimento.

Antes de começar

- Você deve ter permissões de root no diretório **/var/ace** na máquina em que o PAM agent está instalado.
- Confirme se o novo certificado está no formato PEM. Se houver vários certificados CA, eles precisarão ser concatenados em um único arquivo no formato PEM.

  O formato de arquivo deve ser como o seguinte:

  ---BEGIN CERTIFICATE--

  Thawte (BASE64)

  -----END CERTIFICATE-----

  ---BEGIN CERTIFICATE--

  Entrust (BASE64)

  -----END CERTIFICATE-----

Procedimento

1. Renomeie o novo certificado raiz para que ele tenha o mesmo nome que o certificado que você está substituindo.
2. Na máquina onde PAM agent está instalado, copie e substitua ***new_cert_file*.pem** no diretório **/var/ace/**.

Alterando o modo de autenticação do PAM Agent

Você pode alterar o modo de autenticação do PAM agent. Por exemplo, você poderá alterar o modo se quiser usar as opções de autenticação expandida que são fornecidas pelo Serviço de autenticação da nuvem. Por padrão, um PAM agent que recebeu upgrade usa o RSA Authentication Manager com o protocolo UDP.

Alterar do protocolo UDP para o protocolo REST

Você pode alterar o modo de autenticação via protocolo UDP para o protocolo REST no RSA SecurID Authentication Agent 8.1 for PAM ou no Serviço de autenticação da nuvem.

Antes de começar

- Você deve ter permissões de root na máquina em que o agente está instalado.
- Você deve ter permissão de gravação no diretório onde o arquivo **sdconf.rec** está armazenado. Por padrão, esse arquivo é armazenado em **/etc**.
- Você deve ter permissão de gravação no diretório onde o arquivo **mfa_api.properties** está armazenado. Por padrão, esse arquivo é armazenado em **/var/ace/conf**.
- Colete as informações necessárias.

  Para a autenticação no Authentication Manager com o protocolo REST, peça ao Super Admin do Authentication Manager as informações a seguir.

Parâmetro	Descrição
REST_URL	URL do servidor REST para a comunicação entre o agente de autenticação e a instância primária do Authentication Manager. Use o seguinte formato: `https://HOSTNAME:PORT_NO/mfa/v1_1/authn` Na instância primária, obtenha o valor de *HOSTNAME* do campo **Nome do domínio completo** na página **Administração > Rede > Configurações de rede do dispositivo** do Console de operações. A *PORTA* padrão é 5555.
REPLICA_*number* Onde *number* é um valor de 1 a 15.	Uma URL do servidor REST para cada instância de réplica que pode ser usada para failover. Use o seguinte formato: `https://HOSTNAME:PORT_NO/mfa/v1_1/authn` Na instância de réplica, obtenha o valor de *HOSTNAME* do campo **Nome do domínio completo** na página **Administração > Rede > Configurações de rede do dispositivo** do Console de operações. A *PORTA* padrão é 5555.
CLIENT_KEY	Chave de acesso (chave de client) para aprovar com segurança as solicitações de autenticação de usuário no Authentication Manager. Esse valor é gerado no Console de segurança, na instância primária do Authentication Manager.

Parâmetro	Descrição
	Para instruções sobre como obter a chave de acesso, consulte o tópico a seguir no link da RSA: Configurar a API do RSA SecurID Authentication para agentes de autenticação.
CA_CERT_FILE_PATH	Diretório e nome do arquivo para o certificado confiável do servidor no agente de autenticação. O valor padrão é **/var/ace/cert.pem**.
CLIENT_ID	Nome do agente de autenticação (ID do client) que foi criado para o PAM agent no Authentication Manager.

Para a autenticação no Serviço de autenticação da nuvem, peça ao Super Admin do Serviço de autenticação da nuvem as informações a seguir.

Parâmetro	Descrição
REST_URL	URL do servidor REST para a comunicação entre o agente e o Serviço de autenticação da nuvem. Use o seguinte formato: `https://`*`HOSTNAME`*`:`*`PORT`*`/mfa/v1_1/authn` Para o Serviço de autenticação da nuvem, obtenha o valor de *`HOSTNAME`* do campo **Domínio do serviço de autenticação** na guia **Registro** da página de configurações de qualquer roteador de identidade no Cloud Administration Console. A *`PORTA`* padrão é 443.
CLIENT_KEY	Chave da API de autenticação (chave do client) criada no Cloud Administration Console para aprovar com segurança as solicitações de autenticação de usuário no Serviço de autenticação da nuvem. Para instruções sobre como obter a chave da API de autenticação, consulte o tópico a seguir no link da RSA: Adicionar uma chave de API do RSA SecurID Authentication.
CA_CERT_FILE_PATH	Informe o diretório e o nome do arquivo para o certificado confiável do servidor no agente de autenticação. O valor padrão é **/var/ace/cert.pem**.
TENANT_ID	ID do tenant do Serviço de autenticação da nuvem. O PAM agent pode fornecer o ID do tenant em solicitações de autenticação, mas o agente não valida os dados. Atualmente, não há suporte para este parâmetro no Serviço de autenticação da nuvem.
ASSURANCE_POLICY_ID	Nome da política de acesso do Serviço de autenticação da nuvem.
CLIENT_ID	Nome do agente de autenticação a ser exibido nas notificações móveis. Você pode informar qualquer valor. Por exemplo, PAM_Agent.

Procedimento

1. Altere para o diretório onde **sd_pam.conf** está localizado. O local padrão é **/etc**.
2. Abra **sd_pam.conf**.
3. Altere o parâmetro OPERATION_MODE:
   - Para o Authentication Manager com o protocolo REST, digite 1.
   - Para o Serviço de autenticação da nuvem com o protocolo REST, digite 2.

   Se o parâmetro OPERATION_MODE for 0 ou não estiver especificado nem comentado, o PAM agent será padronizado com o modo UDP.

4. Altere para o diretório **/var/ace/conf**. Você precisa atualizar o arquivo **mfa_api.properties**.
5. Abra **mfa_api.properties**.
6. Remova os comentários para habilitar os parâmetros exigidos.
7. Digite um valor para cada parâmetro exigido.
8. Salve o arquivo.

   Agora, você pode usar o protocolo REST.

Depois de concluir

Se o SELinux estiver habilitado, você deverá executar o seguinte comando, em que *REST_port_number* é a porta usada para a autenticação via REST (a porta padrão é 5555):

```
semanage port -a -t dns_port_t -p tcp REST_port_number
```

Alterar do protocolo REST para o protocolo UDP

Depois de instalar o PAM agent para usar o protocolo REST, você pode alterar o modo de autenticação para usar o RSA SecurID Authentication Agent 8.1 for PAM com o protocolo UDP.

Depois que você alterar o modo de autenticação para usar o protocolo UDP, as definições de configuração do protocolo REST no arquivo **mfa_api.properties** não serão mais aplicáveis.

Antes de começar

- O arquivo de configuração do Authentication Manager, **sdconf.rec**, é exigido. Você pode gerar esse arquivo no Authentication Manager ou obter o arquivo com seu Super Admin do Authentication Manager. Para obter mais informações, consulte Planejando-se para instalar o PAM Agent Na página 14.
- Você deve ter permissões de root na máquina em que o agente está instalado e permissão de gravação no diretório onde o arquivo **sd_pam.conf** está armazenado. Por padrão, esse arquivo é armazenado no diretório **/etc**.

Procedimento

1. Altere para o diretório onde **sd_pam.conf** está localizado. O local padrão é **/etc**.
2. Abra **sd_pam.conf**.
3. Altere o parâmetro OPERATION_MODE para 0 para o protocolo UDP:

   ```
   OPERATION_MODE=0
   ```

   Se o parâmetro OPERATION_MODE for 0 ou não estiver especificado nem comentado, o PAM agent será padronizado com o modo UDP.

4. Copie **sdconf.rec** no diretório **/var/ace**.

   Agora, você pode usar o protocolo UDP.

Alterar entre o RSA Authentication Manager e o Serviço de autenticação da nuvem

Você pode alterar se o PAM agent usará o protocolo REST com Authentication Manager ou o Serviço de autenticação da nuvem.

Antes de começar

- Você deve ter permissões de root na máquina em que o agente está instalado.
- Você deve ter permissão de gravação no diretório onde o arquivo **sdconf.rec** está armazenado. Por padrão, esse arquivo é armazenado em **/var/ace**.
- Você deve ter permissão de gravação no diretório onde o arquivo **mfa_api.properties** está armazenado. Por padrão, esse arquivo é armazenado em **/var/ace/conf**.
- O parâmetro CA_CERT_FILE_PATH do certificado confiável do servidor pode permanecer o mesmo. Para os outros parâmetros, colete as informações necessárias:
  Para a autenticação no Authentication Manager com o protocolo REST, peça ao Super Admin do Authentication Manager as seguintes informações:

Parâmetro	Descrição
REST_URL	URL do servidor REST para a comunicação entre o agente de autenticação e a instância primária do Authentication Manager. Use o seguinte formato: `https://HOSTNAME:PORT_NO/mfa/v1_1/authn` Na instância primária, obtenha o valor de *HOSTNAME* do campo **Nome do domínio completo** na página **Administração > Rede > Configurações de rede do dispositivo** do Console de operações. A *PORTA* padrão é 5555.
REPLICA_*number* Onde *number* é um valor de 1 a 15.	Uma URL do servidor REST para cada instância de réplica que pode ser usada para failover. Use o seguinte formato: `https://HOSTNAME:PORT_NO/mfa/v1_1/authn` Na instância de réplica, obtenha o valor de *HOSTNAME* do campo **Nome do domínio completo** na página **Administração > Rede > Configurações de rede do dispositivo** do Console de operações. A *PORTA* padrão é 5555.
CLIENT_KEY	Chave de acesso (chave de client) para aprovar com segurança as solicitações de autenticação de usuário no Authentication Manager. Esse valor é gerado no Console de segurança, na instância primária do Authentication Manager. Para instruções sobre como obter a chave de acesso, consulte o tópico a seguir no link da RSA: Configurar a API do RSA SecurID Authentication para agentes de autenticação.
CLIENT_ID	Nome do agente de autenticação (ID do client) que foi criado para o PAM agent no Authentication Manager.

Para a autenticação no Serviço de autenticação da nuvem, peça ao Super Admin do Serviço de autenticação da nuvem as seguintes informações:

Parâmetro	Descrição
REST_URL	URL do servidor REST para a comunicação entre o agente e o Serviço de autenticação da nuvem. Use o seguinte formato: `https://HOSTNAME:PORT/mfa/v1_1/authn` Para o Serviço de autenticação da nuvem, obtenha o valor de *HOSTNAME* do campo **Domínio do serviço de autenticação** na guia **Registro** da página de configurações de qualquer roteador de identidade no Cloud Administration Console. A *PORTA* padrão é 443.

Parâmetro	Descrição
CLIENT_KEY	Chave da API de autenticação (chave do client) criada no Cloud Administration Console para aprovar com segurança as solicitações de autenticação de usuário no Serviço de autenticação da nuvem. Para instruções sobre como obter a chave da API de autenticação, consulte o tópico a seguir no link da RSA: Adicionar uma chave de API do RSA SecurID Authentication.
TENANT_ID	ID do tenant do Serviço de autenticação da nuvem. O PAM agent pode fornecer o ID do tenant em solicitações de autenticação, mas o agente não valida os dados. Atualmente, não há suporte para este parâmetro no Serviço de autenticação da nuvem.
ASSURANCE_POLICY_ID	Nome da política de acesso do Serviço de autenticação da nuvem.
CLIENT_ID	Nome do agente de autenticação a ser exibido nas notificações móveis. Você pode informar qualquer valor. Por exemplo, PAM_Agent.

Procedimento

1. Altere para o diretório onde **sd_pam.conf** está localizado. O local padrão é **/etc**.
2. Abra **sd_pam.conf**.
3. Altere o parâmetro OPERATION_MODE:
   - Para o Authentication Manager com o protocolo REST, digite 1.
   - Para o Serviço de autenticação da nuvem com o protocolo REST, digite 2.

   Se o parâmetro OPERATION_MODE for 0 ou não estiver especificado nem comentado, o PAM agent será padronizado com o modo UDP.
4. Altere para o diretório **/var/ace/conf**. Você deve atualizar os valores exigidos para os parâmetros no arquivo **mfa_api.properties**.
5. Abra **mfa_api.properties**.
6. Remova os comentários para habilitar os parâmetros exigidos e elimine os comentários de quaisquer parâmetros que não sejam mais necessários.
7. Digite um valor para cada parâmetro exigido.
8. Salve o arquivo.

   Agora, você pode usar o protocolo REST com o novo modo de autenticação.

Apêndice A: Solução de problemas

Problemas de configuração conhecidos

Esta seção descreve os problemas conhecidos.

Problemas com ferramentas compatíveis

Ferramenta	Problema conhecido
dtlogin	**Problema:** as limitações de exibição podem causar dois problemas aos usuários: • Os usuários sendo autenticados não conseguem ver a mensagem completa sobre os métodos de autenticação disponíveis. • Os usuários de senha de reserva podem ver um campo de entrada de texto parcial em telas onde ele não é necessário. **Solução:** os usuários sendo autenticados podem pressionar ENTER, como instruído na tela, para ver a mensagem completa. Os usuários de senha de reserva podem ignorar o campo desnecessário.
ftp	• **Problema:** quando você usa o SecurID para proteger o ftp, as solicitações de autenticação do SecurID e as mensagens de erro não são exibidas aos usuários. Apenas as mensagens de erro e os prompts padrão do SO são exibidos. **Solução:** oriente os usuários a digitar o respectivo nome de usuário no prompt de nome de usuário do SO e o passcode do SecurID no prompt de senha do SO. Se um usuário não souber o status do token (por exemplo, se o token está no modo de próximo tokencode ou no modo de novo PIN), ele deverá fazer a autenticação com outra ferramenta de conexão, como rlogin, para verificar se o PIN ou tokencode ainda é válido. • O FTP não comporta o atraso de retirada exponencial. • Não é possível usar o Serviço de autenticação da nuvem para proteger o ftp. No entanto, o sftp é aceito.
ssh	**Problema:** depois que um usuário faz três tentativas de autenticação sem sucesso no SecurID em uma única sessão, a conexão é encerrada. **Solução:** o usuário pode encerrar a sessão e iniciar outra sessão.
ftp com SELinux	**Problema:** quando o SELinux está habilitado, o usuário da ferramenta de ftp vê a mensagem "500 OOPS: cannot change directory:/home/tzfFjG_9su." **Solução:** na máquina do agente, execute o comando "setsebool -P ftp_*home_dir* on", onde *home_dir* é o diretório de usuário.
gdm	**Problema:**PAM agent as mensagens podem ficar truncadas. **Solução:** o tema de gdm pode ser configurado adequadamente para evitar esse problema.
rlogin	**Problema:** no RHEL 6.8, antes que o rlogin seja configurado para funcionar com o PAM agent, as conexões de rlogin são encerradas. **Solução:** certifique-se de que rlogin funcione antes de configurar o PAM agent. Siga estas etapas: 1. Abra o arquivo **/etc/xinet,d/rlogin**. 2. Adicione **nice = 5** ao final da configuração de rlogin. 3. Reinicie os serviços de xinetd: `service xinetd restart`

Ferramenta	Problema conhecido
rlogin	**Problema:** no Oracle Linux 6.8, rlogin não funciona. **Solução:** faça downgrade para o seguinte rpms: **util-linux-ng-2.17.2-12.18.el6.x86_64.rpm** **libblkid-2.17.2-12.18.el6.x86_64.rpm** **libuuid-2.17.2-12.18.el6.x86_64.rpm**
rlogin	**Problema:** se a primeira tentativa de processar uma solicitação de rlogin falhar, a sessão será transmitida ao daemon de log-in. **Solução:** se configurar o Linux para usar rlogin, você deverá configurar o arquivo de log-in remoto em **/etc/pam.d**.
rlogin	**Problema:** rlogin solicita uma senha em vez de um passcode quando entradas ambíguas estão presentes no arquivo **/etc/hosts**. **Solução:** se existir um nome de máquina ao lado do endereço IP de loopback e do endereço real da máquina, remova o nome da máquina ao lado do endereço IP de loopback para que rlogin tenha o comportamento esperado.
rlogin	**Problema:** quando um usuário tenta acessar o sistema usando a ferramenta rlogin e digita as credenciais erradas, o sistema redireciona o processo de autenticação para a ferramenta telnet, além de solicitar uma senha ou um passcode, conforme a configuração de telnet. **Solução:** quando o rlogin é protegido pelo SecurID, o telnet também deve ser protegido pelo SecurID e vice-versa.

Problemas de upgrade e desinstalação

Problema: Se tentar fazer upgrade ou desinstalar o PAM agent sem desabilitar o módulo PAM da RSA, você poderá ver a mensagem de erro: "pam_securid.so is busy, not able to remove/replace".
Solução: Para resolver esse problema, você deve fazer log-on com ferramentas diferentes de ssh e remover o arquivo **pam_securid.so**.

Utilitários de autenticação para o modo UDP

Os utilitários de autenticação estão localizados nos seguintes diretórios:

- sistema operacional de 32 bits: ***pam agent installation directory*/bin/32bit**
- sistema operacional de 64 bits: ***pam agent installation directory*/bin/64bit**

Use esses utilitários para:

- Fazer um teste de autenticação. Para obter mais informações, consulte Executar o utilitário acetest abaixo.
- Verificar a comunicação entre o PAM agent e o RSA Authentication Manager. Para obter mais informações, consulte Executar o utilitário acestatus Na página seguinte.

Você pode habilitar o registro para esses utilitários. Para obter mais informações, consulte Habilitar o registro de rastreamento do SecurID para o modo UDP Na página 29

Executar o utilitário acetest

Este utilitário verifica se o agente está funcionando adequadamente ao fazer um teste de autenticação.

Procedimento

1. Altere para o diretório de utilitários de autenticação do PAM agent.
   - sistema operacional de 32 bits: ***pam agent installation directory*/bin/32bit**
   - sistema operacional de 64 bits: ***pam agent installation directory*/bin/64bit**
2. Digite:

   ```
   ./acetest
   ```

3. Digite o nome de usuário válido e o passcode.

Se o acesso lhe for negado repetidamente, teste a conectividade com o servidor do Authentication Manager usando o utilitário Executar o utilitário acestatus abaixo ou entre em contato com seu administrador do Authentication Manager.

Executar o utilitário acestatus

Este utilitário verifica o status de cada Authentication Manager onde o PAM agent está registrado como um host de agente. Se você tiver dúvidas sobre as informações exibidas, entre em contato com seu administrador do Authentication Manager.

Procedimento

1. Altere para o diretório de utilitários do PAM agent.
2. Digite:

   ```
   ./acestatus
   ```

A tabela a seguir lista as informações exibidas na seção do Authentication Manager.

Informações retornadas	**Descrição**
Versão da configuração	Versão do arquivo **sdconf.rec** que está em uso. Para o RSA Authentication Manager 8.0 ou posterior, esse número é 14.
Habilitado para DES	Se o ambiente de configuração aceitar protocolos pré-existentes, YES será exibido.
Repetições de client	Número de vezes em que o PAM agent envia dados de autenticação para o Authentication Manager antes que ocorra um timeout.
Timeout do client	Tempo (em segundos) que o PAM agent aguarda antes de reenviar os dados de autenticação para o Authentication Manager.
Versão do servidor	Número da versão do Authentication Manager.
Comunicação	Versão do protocolo usado pelo Authentication Manager e pelo PAM agent.

A tabela a seguir lista as informações de status exibidas na seção do Authentication Manager.

Informações de status	**Descrição**
Endereço do servidor ativo	O endereço IP que o PAM agent usa para se comunicar com o servidor. Esse endereço pode ser o endereço IP real do servidor que você selecionou ou um endereço IP de alias atribuído ao servidor. Um endereço IP igual a 0.0.0.0 indica que o agente ainda não recebeu a comunicação do servidor.

A tabela a seguir lista as informações de status do servidor exibidas na seção do Authentication Manager.

Status do servidor	Descrição
Disponível para autenticações	Este servidor está disponível para lidar com as solicitações de autenticação.
Não utilizado	O servidor ainda não recebeu uma solicitação de autenticação.
Somente para failover	O servidor está reservado somente para uso de failover.
Servidor padrão durante solicitações inicias	Somente este servidor está disponível para lidar com as solicitações neste momento.

Utilitário de conversão para o modo UDP

O utilitário de conversão é usado quando um PAM agent baseado em UDP (User Datagram Protocol) coexiste com outros agentes do SecurID.

O utilitário de conversão ns_conv_util está localizado nos seguintes diretórios:

- sistema operacional de 32 bits: ***pam agent home*/bin/32bit**
- sistema operacional de 64 bits: ***pam agent home*/bin/64bit**

Procedimento

1. Altere para o diretório de utilitários do PAM agent.
2. Digite:

   `./ns_conv_util <Existing_Securid_file_path> <New_Securid_dir_path>`

   onde *<Existing_Securid_file_path>* é o caminho onde existe o arquivo atual do SecurID,

   e *<New_Securid_dir_path>* é o diretório onde o arquivo recém-gerado do SecurID deve ser armazenado.

   Por exemplo:

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

3. Se o novo local de destino não for o mesmo local especificado por VAR_ACE, copie o novo arquivo do SecurID nesse local.

Segredos do nó para o modo UDP

O segredo do nó é uma chave de criptografia simétrica que RSA Authentication Manager e o PAM agent usam para criptografar e descriptografar pacotes de dados enquanto eles viajam através da rede. Os segredos de nó são necessários para os agentes que utilizam o protocolo UDP. O segredo do nó compartilhado é armazenado no banco de dados do Authentication Manager e em um arquivo na máquina em que o PAM agent está instalado. Para os agentes que usam o protocolo REST, um arquivo de segredo do nó não é usado. Em vez de um segredo do nó, uma chave negociada dinamicamente é usada para criptografar o canal, juntamente com um algoritmo forte de criptografia.

Para agentes baseados em UDP, se o segredo do nó estiver ausente no servidor do Authentication Manager ou na máquina em que o PAM agent está instalado, limpe o segredo do nó no outro local. Se os arquivos de segredo do

nó no Authentication Manager e na máquina do PAM agent não forem correspondentes, limpe o segredo do nó nos dois locais. Depois de limpar o segredo do nó, você deve gerar um novo segredo do nó.

Limpar o segredo do nó do RSA SecurID Authentication Agent 8.1 for PAM

Se o segredo do nó não for correspondente no RSA SecurID Authentication Agent 8.1 for PAM e na máquina em que o PAM agent está instalado ou se o segredo do nó estiver ausente da máquina do PAM agent, você deverá limpar o segredo do nó do Authentication Manager. Por exemplo, se você reinstalar o PAM agent, o segredo do nó estará ausente da máquina do PAM agent.

Procedimento

1. No Console de segurança do Authentication Manager, clique em **Acessar > Agentes de autenticação > Gerenciar existentes**.
2. Localize a máquina do agente afetado e selecione **Gerenciar segredo do nó** no menu drop-down.
3. Marque a caixa de seleção **Limpar o segredo do nó** e, em seguida, clique em **Salvar**.

Depois de concluir

- Se houver um segredo do nó na máquina do PAM agent, consulte Limpar o segredo do nó da máquina do PAM Agent abaixo.
- Se a máquina do PAM agent não tiver um segredo do nó, siga o procedimento Gerar um novo segredo do nó abaixo.

Limpar o segredo do nó da máquina do PAM Agent

Se o segredo do nó não for correspondente na instância do RSA Authentication Manager e na máquina do PAM agent ou se o segredo do nó estiver ausente do Authentication Manager, você deverá limpar o segredo do nó da máquina do PAM agent. Por exemplo, se você instalar uma nova instância do Authentication Manager e adicionar um PAM agent existente, o segredo do nó estará ausente do Authentication Manager.

Antes de começar

Se houver um segredo do nó no Authentication Manager, consulte Limpar o segredo do nó do RSA SecurID Authentication Agent 8.1 for PAM acima.

Procedimento

1. Faça log-on na máquina em que o PAM agent está instalado e localize **securid**, o arquivo de segredo do nó, no diretório **/var/ace**.
2. Renomeie ou exclua o arquivo de segredo do nó.
3. O segredo do nó também é armazenado no cache do servidor. Reinicie a máquina para limpar o segredo do nó do cache.

Depois de concluir

Gerar um novo segredo do nó abaixo

Gerar um novo segredo do nó

Procedimento

1. Execute o utilitário acetest a partir da máquina do PAM agent para gerar o arquivo de segredo do nó. Para obter mais informações, consulte Utilitários de autenticação para o modo UDP Na página 41.

2. Verifique os registros de autenticação e certifique-se de que um novo segredo do nó tenha sido enviado.
3. Reinicie sua máquina do PAM agent para que o agente possa ler o arquivo de segredo do nó.

Registro do PAM Agent

Se o registro estiver habilitado, por padrão, as mensagens de autenticação do PAM agent serão gravadas no log do sistema. Para fins de rastreamento, você pode configurar o log do sistema para gravar mensagens de log de autenticação do PAM agent para ferramentas específicas. Consulte Habilitar a saída de depuração Na página 28.

Configurar o log do sistema

O procedimento a seguir envia todas as mensagens de autenticação ao log do sistema.

Procedimento

1. Altere para o diretório **/etc/**.
2. Abra o arquivo **syslog.conf**.
3. Adicione o parâmetro `auth.notice` à linha que especifica o arquivo de log do sistema.
4. Remova o parâmetro `authpriv.none` se ele estiver especificado para o arquivo de log do sistema.
5. Se você estiver usando telnet ou login, adicione o parâmetro `authpriv.notice` à linha que especifica o arquivo de log do sistema.
6. Salve suas alterações.
7. Reinicie o daemon do syslog.

Mensagens de log de autenticação do PAM Agent

A tabela a seguir lista as mensagens de log de autenticação.

Mensagem	Descrição
Cannot locate **sd_pam.conf** file	O arquivo de configuração **sd_pam.conf** não está no diretório **/etc**; **/etc** deve conter o arquivo de configuração correto para que VAR_ACE possa ser definido adequadamente.
AceInitialize failed	AceInitialize é uma chamada de função de API que inicializa threads de operador e carrega as definições de configuração do **sdconf.rec**. Verifique se você tem a cópia mais recente do **sdconf.rec** com seu administrador do Authentication Manager e se VAR_ACE está definido corretamente.
Cannot communicate with RSA ACE/Server	Os intermediadores do Authentication Manager não foram iniciados ou houve uma falha de rede. Contate o administrador do Authentication Manager ou o administrador de rede.
Reserve password exceeds character limit	O limite máximo é de 256 caracteres.
Invalid reserve password	A senha de reserva é a mesma senha do sistema para o host. Você deverá saber essa senha se o Authentication Manager conseguir processar as solicitações de autenticação.
User name exceeds character limit	O nome de usuário não deve exceder 31 caracteres.

Mensagem	Descrição
Reserve password not allowed. User is not root.	Verifique se você é um usuário root. Somente os usuários root podem usar a senha de reserva.

Registro para o modo REST

O modo REST comporta registros adicionais implementados com a biblioteca **log4cxx**. O registro da camada REST é separado dos registros do PAM agent. RollingFileAppender e SyslogAppender são aceitos. Por padrão, RollingFileAppender é habilitado. Os registros são enviados para **/var/ace/log/mfa_rest.log** com o nível de registro definido como INFO. O rodízio com base no tamanho está habilitado com um tamanho de rodízio de 10 MB.

O rodízio de registros com base em tempo não é aceito. As ferramentas compatíveis, como ssh e su, carregam o agente de autenticação para todas as solicitações e, portanto, o PAM agent não consegue alternar os registros com base no tempo. O PAM agent aceita o rodízio de registros com base no tamanho.

Você pode alterar as configurações de registro padrão para o modo REST.

Procedimento

1. Altere para o diretório **/var/ace/conf**.
2. Abra o arquivo **log.properties**.
3. Configure as seguintes entradas para o rodízio com base no tamanho:

   ```
   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. Configure as seguintes entradas para dar suporte ao registro local e remoto do 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. Salve suas alterações.
6. Reinicie o daemon do syslog.

Solução de problemas do SELinux

Às vezes, o SELinux (Security-Enhanced Linux) exige procedimentos adicionais, conforme especificado abaixo.

Usando o protocolo REST em um agente de upgrade

Para usar o protocolo REST na autenticação, você deve sobregravar a política do SELinux existente quando você faz upgrade do PAM agent. Caso contrário, algumas ferramentas não conseguirão fazer a autenticação com o protocolo REST.

Para atualizar a política do SELinux, você pode executar o script de instalação novamente e sobregravar a política existente. Os arquivos que já receberam upgrade não serão afetados.

Habilitar as configurações de caminho personalizado

Quando o SELinux está habilitado, as configurações de caminho personalizado para VAR_ACE e RSATRACEDEST não funcionam por padrão.

Procedimento

Para habilitar as configurações de caminho personalizado, você deve digitar os seguintes comandos, onde *<custom_directory_path>* é o caminho do arquivo do diretório VAR_ACE personalizado ou do diretório RSATRACEDEST que você deseja usar:

```
semanage fcontext -a -t var_t <custom_directory_path>

restorecon -R <custom_directory_path>
```

Configurar os valores de timeout e repetição para a autenticação REST

Você pode configurar quanto tempo o PAM agent pode demorar para se conectar com o RSA Authentication Manager ou o Serviço de autenticação da nuvem e por quanto tempo o PAM agent aguardará uma resposta. Você também pode configurar o número de vezes que o PAM agent tenta contatar uma instância primária ou de réplica do Authentication Manager ou o Serviço de autenticação da nuvem. Esses parâmetros são usados apenas pelo protocolo REST.

Lembre-se de considerar a velocidade de sua rede. Definir valores altos de timeout em uma rede mais lenta permite que a autenticação seja bem-sucedida.

Antes de começar

Você deve ter permissões de root na máquina em que o agente está instalado e permissão de gravação no diretório onde o arquivo **mfa_api.properties** está armazenado. Por padrão, esse arquivo é armazenado em **/var/ace/conf**.

Procedimento

1. Altere para o diretório onde **mfa_api.properties** está localizado. Por padrão, o diretório é **/var/ace/conf**.
2. Abra **mfa_api.properties**.
3. Os seguintes parâmetros podem ser alterados:
   - CONNECT_TIMEOUT. O número máximo de segundos permitidos para o agente se conectar com o servidor. O padrão é 60 segundos.
   - READ_TIMEOUT. O número máximo de segundos permitidos para se conectar com o servidor e ler a resposta. O valor de READ_TIMEOUT deve ser igual à soma do valor de CONNECT_TIMEOUT e do tempo máximo permitido para ler a resposta. O padrão é 120 segundos.
   - MAX_RETRIES. O número de vezes que o PAM agent tenta se conectar com o Authentication Manager ou o Serviço de autenticação da nuvem. O valor padrão é 3.
   - Para a fase de inicialização da interface REST do Authentication Manager, quando o PAM agent inicia uma tentativa de autenticação, MAX_RETRIES é o número de vezes que o agente tenta contatar o mesmo servidor antes do failover para outro servidor. Durante a fase de verificação, quando o PAM agent está fornecendo as credenciais de autenticação, o failover não é aceito, e MAX_RETRIES é o número de vezes que o agente tenta contatar o mesmo servidor antes da falha da autenticação.
   - O Serviço de autenticação da nuvem não comporta o failover. Nas fases de inicialização e verificação, MAX_RETRIES é o número de vezes que o agente tenta contatar o mesmo servidor antes da falha da autenticação.
4. Salve o arquivo.

Desinstalar o RSA Authentication Agent 8.1 for PAM

Você pode desinstalar manualmente o PAM agent em máquinas individuais ou pode optar por desinstalar de modo silencioso e automático várias cópias do PAM agent.

A desinstalação do RSA Authentication Agent 8.1 for PAM remove os rótulos SELINUX configurados para as bibliotecas REST que foram criadas durante a instalação do PAM agent.

Antes de começar

- Configure as ferramentas protegidas do RSA SecurID para que usem o módulo de PAM padrão fornecido com seu sistema operacional, e não o módulo de PAM da RSA. Todas as sessões ativas que usam os módulos de PAM da RSA deverão ser fechadas antes de você continuar com a desinstalação. Você deve desfazer os procedimentos que seguiu em Configurando ferramentas Na página 24.

  Obs.: se desinstalar o módulo da RSA enquanto houver referências ao módulo da RSA no diretório **/etc/pam.d**, você ficará bloqueado fora de seu sistema.

- Verifique se você tem permissões de root no host.

Desinstalar o PAM Agent de uma máquina

Execute esta tarefa para desinstalar um PAM agent.

Procedimento

1. Altere para o diretório de usuário do PAM agent. Por exemplo, **/opt/pam**.
2. Execute o script de desinstalação. Digite:

   ```
   ./uninstall_pam.sh
   ```

3. Verifique se o diretório de instalação foi removido. Se o diretório ainda existir, você deverá removê-lo manualmente.
4. Para verificar se o PAM agent foi removido com sucesso, verifique o arquivo **/var/pam_uninstaller/uninstaller.log**.

Desinstalação em massa do PAM Agent no modo silencioso

Execute esta tarefa para desinstalar um grande número de PAM agents.

Procedimento

1. Crie um arquivo de configuração com base em texto com o nome **unconfig**. O arquivo deve conter as seguintes informações:

   ```
   y
   y
   y
   ```

   Cada y é uma resposta a um prompt:

   - Are you sure that you would like to uninstall the RSA Authentication Agent 8.1.0 [101] for PAM?
   - O RSA Authentication Agent for PAM será excluído do diretório <*install_path*>. 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. Altere para o diretório de usuário do PAM agent. Por exemplo, **/opt/pam**.
3. Execute o script de desinstalação. Digite:

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

Apêndice B: Arquivos de configuração essenciais

Arquivos de configuração essenciais

O diretório de instalação padrão do PAM agent é **/opt/pam**, e isso pode ser alterado durante a instalação. Por padrão, o diretório **/var/ace** inclui bibliotecas e arquivos relacionados a REST. O local desse diretório não pode ser alterado.

Além dos binários (**pam_securid.so**, **acetest**, **acestatus** e **ns_conv_util**), o PAM agent mantém os arquivos de configuração essenciais listados na tabela a seguir.

Arquivo	Descrição
log.properties	Arquivo de configuração de registro do PAM agent para o protocolo REST. O PAM agent usa a biblioteca **log4cxx** para o registro no modo REST.
mfa_ api.properties	Contém as configurações utilizadas pelo protocolo REST para a autenticação no Authentication Manager e no Serviço de autenticação da nuvem.
sdconf.rec	Esse arquivo é gerado pelo RSA Authentication Manager e contém a informação sobre configuração que controla o comportamento do PAM Agent. A permissão desse arquivo deve ter o root de root -rw-------. Esse arquivo é usado apenas no modo UDP.
sdopts.rec	Esse arquivo é usado para o balanceamento de carga manual. Ele contém uma lista de endereços IP para instâncias do Authentication Manager. A permissão desse arquivo deve ter o root de root -rw-------. Esse arquivo é usado apenas no modo UDP.
sdstatus.12	Esse arquivo é gerado pela API de autenticação do PAM agent para rastrear o último status conhecido dos servidores do Authentication Manager. A permissão desse arquivo deve ter o root de root -rw-------.
sd_pam.conf	Contém as definições de configuração que controlam o comportamento do PAM agent. A permissão desse arquivo deve ter o root de root -rw-r--r--.
securid	Este arquivo contém uma chave secreta compartilhada usada para proteger a comunicação via protocolo UDP entre a máquina local e o Authentication Manager. O nome desse arquivo é oriundo do nome do protocolo configurado no sistema local para a porta pela qual o agente se comunica com o Authentication Manager, normalmente por meio do arquivo de "serviço". A permissão desse arquivo deve ter o root de root -r--------. No entanto, isso também depende da configuração de Umask do SO. O protocolo UDP exige esse arquivo. Esse arquivo é opcional para a autenticação com o protocolo REST.