**Guia IBM Connect:Direct UNIX Autenticação com PAM**

**Exemplo de Autenticação com PAM**

2025 - Versão 1.0

IBM Corporation

Sumário

[1. O que é PAM 3](#_Toc196311567)

[PAM - Pluggable Authentication Modules 3](#_Toc196311568)

[2. Escopo 4](#_Toc196311569)

[3. Autenticação usando grupo local. 5](#_Toc196311570)

[Grupo e Usuarios Linux 5](#_Toc196311571)

[Configuração do PAM 6](#_Toc196311572)

[Configuração do IBM Connect:Direct 7](#_Toc196311573)

# 1. O que é PAM

## PAM - Pluggable Authentication Modules

É um sistema modular de autenticação usado no Linux (e Unix), que permite controlar como usuários se autenticam no sistema.

O PAM possui um conjunto de bibliotecas que permite que um administrador de sistema Linux configure métodos para autenticar usuários.

Ele fornece uma maneira flexível e centralizada de alternar métodos de autenticação para aplicativos seguros usando arquivos de configuração em vez de alterar o código do aplicativo.

Linux-PAM separa as tarefas de autenticação em quatro *Module Types*:

| **Module Types** | **Função** |
| --- | --- |
| auth | Autenticação (login, senha) |
| account | Controle de acesso (horário, grupo) |
| password | Atualização de senha |
| session | Ações durante login/logout |

Os “*Module Types*” são as funcoes de autenticação que usam as implementaçoes de modulo.

Exemplo de implementacoes de modulo:

* pam\_unix – Autenticação baseada em arquivos do sistema, como /etc/passwd e /etc/shadow.
* pam\_tally – Contabilização de tentativas de login.
* pam\_google\_authenticator – Autenticação de dois fatores usando o Google Authenticator.
* pam\_ldap – Autenticação usando LDAP.
* pam\_radius – Autenticação através de RADIUS.
* pam\_succeed\_if – Condições para autenticação com base em variáveis do sistema.
* pam\_env – Definição de variáveis de ambiente durante o processo de login.
* pam\_group – Verifica a associação a grupos para a autenticação.
* pam\_nologin – Impede login quando o arquivo /etc/nologin existe.

Em reusmo

O “***Module Types****”* são as fases do processo de autenticação (auth, account, password e session).

O ***“module”*** são as implementações específicas que fazem o trabalho dentro dessas fases (como pam\_unix.so, pam\_ldap.so, pam\_tally.so, etc.).

# 2. Escopo

Este documento não aborda as configurações avançadas do PAM, apresenta apenas um exemplo básico de utilização do PAM em conjunto com o IBM Connect:Direct.

Este documento descreve os procedimentos para configurar o autenticador do IBM Connect:Direct para utilizar o PAM.

A configuração do PAM é uma tarefa geralmente atribuída à equipe de administração do sistema operacional e são procedimentos utilizando um usuario administrador.

# 3. Autenticação usando grupo local.

## Grupo e Usuarios Linux

##### Criar um grupo local

A black background with white text

AI-generated content may be incorrect.

groupadd cdadmingrp

##### Criar um usuario local



useradd cdusuariopam

echo "senha" | passwd --stdin cdusuariopam

##### Atriuir o usuario ao Grupo



usermod -aG cdadmingrp cdusuariopam

##### Listar usuarios do grupo

A black background with white text

AI-generated content may be incorrect.

getent group cdadmingrp

## Configuração do PAM

##### Verificar versao do PAM utilizada no teste v1.3.1

A computer screen shot of a program

AI-generated content may be incorrect.

1. Criar um servico chamado “**cdlogin**” no diretorio do PAM (criar um arquivo):

Acessar diretorio do PAM

A black background with white text

AI-generated content may be incorrect.

Criar um arquivo dentro do diretorio chamado “**cdlogin**”

A screen shot of a computer

AI-generated content may be incorrect.

Exemplo:

#%PAM-1.0

# Exemplo de Servico de autenticacao /etc/pam.d/cdlogin

# Autenticação simples usando contas locais

auth required pam\_unix.so

# Verifica se a conta existe no grupo de acesso “**cdadmingrp**”

account required pam\_succeed\_if.so user ingroup cdadmingrp

# Permite alteração de senha (caso necessário)

password required pam\_unix.so

# Inicia uma sessão básica

session required pam\_unix.so

## Configuração do IBM Connect:Direct

1. Configurar no arquivo “initparm.cfg” o servico “CDlogin” do PAM

Editar o arquivo “*<dir-install-cd>/ndm/cfg/<nodename>/initparm.cfg*”

Localizar o parametro “*ndm.pam:service*”

Informar o servico PAM “**cdlogin**”

*# Miscellaneous Parameters*

*ndm.pam:\*

*:service=cdlogin:*

A screen shot of a computer

AI-generated content may be incorrect.

1. Editar o arquivo “userfile.cfg” e informar o usuario do grupo

A screenshot of a computer

AI-generated content may be incorrect.

userfile.cfg

…

**cdusuariopam**:\

:admin.auth=y:\

:pstmt.copy.ulimit=y:\

:pstmt.upload=y:\

:pstmt.download=y:\

:name=None:\

:client.cert\_auth=n:\

:cmd.external.stat.log=y:

**A screenshot of a computer program

AI-generated content may be incorrect.**

**Ou**

**\***:\

:admin.auth=y:\

:pstmt.copy.ulimit=y:\

:pstmt.upload=y:\

:pstmt.download=y:\

:name=None:\

:client.cert\_auth=n:\

:cmd.external.stat.log=y:

1. Realizar login pelo no WebService ao Node.

A screenshot of a computer

AI-generated content may be incorrect.

**A screenshot of a computer

AI-generated content may be incorrect.**

**Referencia:**

[**https://www.ibm.com/support/pages/how-implement-pluggable-authentication-module**](https://www.ibm.com/support/pages/how-implement-pluggable-authentication-module)

[**https://www.ibm.com/docs/en/connect-direct/6.4.0?topic=guide-password-storage**](https://www.ibm.com/docs/en/connect-direct/6.4.0?topic=guide-password-storage)