UNIVERSIDAD DE BURGOS
ESCUELA POLITÉCNICA SUPERIOR
Grado en Ingeniería Informática

TFG del Grado en Ingeniería Informática

Implementación de una Prueba de Concepto (PoC) de Manage Engine PAM para la Gestión Eficiente de Acceso Privilegiado en Organizaciones Documentación Técnica

Presentado por Alejandro Villar Solla
en Universidad de Burgos — 10 de junio de 2024
Tutor: Luis Antonio Antolín Sánchez

Índice general

Índice de figuras

Índice de tablas

Apéndice A

Plan de Proyecto Software

A.1. Introducción

Este documento detalla el Plan de Proyecto para la implementación de PAM360 en NTT Data, cubriendo todos los aspectos desde la planificación inicial hasta la finalización del proyecto. El objetivo es proporcionar una guía clara y detallada que asegure el éxito en la implementación y configuración de la herramienta PAM360 para la gestión de accesos privilegiados.

A.2. Objetivos

El objetivo principal de este proyecto es implementar y configurar PAM360 para mejorar la gestión de accesos privilegiados en NTT Data. Los objetivos específicos incluyen:

- Mejorar la seguridad mediante el control y monitoreo de accesos privilegiados.
- Optimizar la eficiencia en la gestión de usuarios y contraseñas.
- Asegurar la transparencia y trazabilidad de las actividades de los usuarios.
- Facilitar la auditoría y el cumplimiento normativo.
- Integrar PAM360 con las infraestructuras existentes de NTT Data.

A.3. Alcance del Proyecto

El alcance del proyecto abarca la instalación, configuración e integración de PAM360 con el Active Directory de NTT Data, incluyendo:

- Revisión de documentación técnica.
- Preparación del entorno de pruebas.
- Despliegue y configuración de PAM360.
- Integración con AD y pruebas funcionales.
- Configuración de políticas de seguridad y contraseñas.
- Generación de reportes y auditorías.
- Formación y capacitación para los administradores del sistema.

A.4. Cronograma

El proyecto se desarrollará en las siguientes fases:

- **Fase 1: Revisión de Documentación** (1 semana)
- **Fase 2: Preparación del Entorno** (1 semanas)
- **Fase 3: Implementación** (1 semanas)
- **Fase 4: Configuración y Pruebas Funcionales** (1 semanas)
- **Fase 5: Evaluación y Análisis** (1 semanas)
- **Fase 6: Documentación Final y Capacitación** (2 semana)

A.5. Recursos

Recursos Humanos

- **Gestor de Proyecto**: Responsable de la coordinación y seguimiento del proyecto.

- **Especialista en Seguridad**: Encargado de la configuración y pruebas de seguridad.
- **Administrador de Sistemas**: Responsable de la integración con AD y gestión de usuarios.

Recursos Materiales y de Software

- Servidores virtuales para pruebas y despliegue.
- Licencias de software para PAM360 y herramientas de virtualización (vSphere, MRemote).
- Documentación técnica y manuales de usuario.
- Equipos de red y hardware de soporte.

A.6. Riesgos y Mitigación

Riesgo	**Mitigación**
Problemas de Integración con AD	Realizar pruebas preliminares en un entorno controlado.
Fallos en la Configuración de PAM360	Contar con el soporte técnico del proveedor y documentación detallada.
Resistencia al Cambio por parte del Personal	Implementar programas de formación y capacitación.
Vulnerabilidades de Seguridad	Actualizar regularmente el software y realizar auditorías de seguridad.
Problemas de Conectividad	Buena configuración en el firewall de permisos y mantenimiento pertinente.

Tabla A.1: Riesgos y Mitigación

A.7. Control y Seguimiento

Para asegurar el cumplimiento de los objetivos del proyecto, se llevarán a cabo las siguientes actividades de control y seguimiento:

- Reuniones semanales de seguimiento con el equipo de proyecto.
- Reportes de avance semanales.

- Evaluaciones periódicas de cumplimiento de hitos.
- Auditorías internas para verificar la correcta implementación y configuración de PAM360.

A.8. Conclusiones

El Plan de Proyecto Software para la implementación de PAM360 en NTT Data establece una guía clara para llevar a cabo todas las fases del proyecto, asegurando una gestión eficiente y segura de los accesos privilegiados en la organización. Con una planificación detallada, asignación adecuada de recursos y mitigación de riesgos, se espera alcanzar todos los objetivos propuestos de manera exitosa. Además, la integración con las infraestructuras existentes y la capacitación del personal son factores clave para el éxito del proyecto y su sostenibilidad a largo plazo.

Apéndice B

Plan de Calidad del Proyecto

B.1. Introducción

El Plan de Calidad del Proyecto establece los procedimientos y estándares necesarios para asegurar que la implementación de PAM360 en NTT Data cumpla con los requisitos de calidad definidos. Este documento detalla las actividades de control de calidad que se llevarán a cabo durante el proyecto.

B.2. Casos de uso

A continuación, se describen los principales casos de uso identificados para la implementación de PAM360:

B.3. Objetivos de Calidad

Los objetivos de calidad del proyecto incluyen:

- Garantizar que PAM360 se instale y configure correctamente según las especificaciones del proveedor y los requisitos de NTT Data.
- Asegurar que todas las funcionalidades de PAM360 se integren y operen sin problemas con el Active Directory de NTT Data.
- Cumplir con los estándares de seguridad y buenas prácticas en la gestión de accesos privilegiados.

CU-1	**Instalación y Configuración de PAM360**
Versión	1.0
Autor	Alejandro Villar Solla
Requisitos asociados	RF-01, RF-02
Descripción	Este caso de uso describe los pasos para instalar y configurar PAM360 en el entorno virtualizado de NTT Data.
Precondición	▪ Entorno virtualizado preparado. ▪ Archivo de instalación de PAM360 disponible.
Acciones	1. Descargar el archivo de instalación de PAM360 desde el sitio web del proveedor. 2. Copiar el archivo .exe a la máquina virtual utilizando MRemote. 3. Ejecutar el instalador y seguir las instrucciones de instalación. 4. Configurar los parámetros iniciales (puertos, credenciales administrativas).
Postcondición	▪ PAM360 instalado y corriendo en localhost:8282. ▪ Acceso a la interfaz web de PAM360.
Excepciones	▪ Error durante la instalación debido a incompatibilidad de SO o errores comunes. ▪ Falta de permisos administrativos para ejecutar el instalador.
Importancia	Alta

Tabla B.1: CU-1 Instalación y Configuración de PAM360.

CU-2	**Integración de PAM360 con Active Directory**
Versión	1.0
Autor	Alejandro Villar Solla
Requisitos asociados	RF-03, RF-04
Descripción	Este caso de uso describe el proceso de integración de PAM360 con el Active Directory (AD) de NTT Data para sincronización de usuarios y roles.
Precondición	▪ PAM360 instalado y configurado. ▪ Acceso administrativo a Active Directory.
Acciones	1. Acceder a la interfaz web de PAM360. 2. Navegar a la configuración de administración y seleccionar İmport From Active Directory". 3. Ingresar el nombre del dominio AD y las credenciales de la cuenta asociada. 4. Seleccionar los usuarios a sincronizar. 5. Confirmar y ejecutar la integración.
Postcondición	▪ Usuarios y roles del AD sincronizados en PAM360. ▪ Accesos privilegiados gestionados centralmente desde PAM360.
Excepciones	▪ Error de autenticación con AD.
Importancia	Alta

Tabla B.2: CU-2 Integración de PAM360 con Active Directory.

CU-3	**Configuración de Políticas de Seguridad en PAM360**
Versión	1.0
Autor	Alejandro Villar Solla
Requisitos asociados	RF-05, RF-06
Descripción	Este caso de uso describe el procedimiento para configurar las políticas de seguridad dentro de PAM360, incluyendo autenticación y gestión de contraseñas.
Precondición	▪ PAM360 instalado y configurado. ▪ Acceso administrativo a la consola de PAM360.
Acciones	1. Iniciar sesión en la consola web de PAM360. 2. Navegar a la sección de configuración de administración. 3. Seleccionar "Políticas de Seguridadz luego "Gestión de Contraseñas". 4. Configurar las reglas de complejidad de contraseñas, frecuencia de cambio y políticas de bloqueo de cuentas. 5. Guardar y aplicar las políticas configuradas.
Postcondición	▪ Políticas de seguridad y contraseñas aplicadas y activas en PAM360. ▪ Refuerzo de la seguridad en la gestión de accesos privilegiados.
Excepciones	▪ Error al guardar las políticas debido a conflictos con configuraciones existentes. ▪ Usuarios no cumplen con las nuevas políticas de contraseña y necesitan soporte.
Importancia	Alta

Tabla B.3: CU-3 Configuración de Políticas de Seguridad en PAM360.

- Obtener retroalimentación y aprobación de los usuarios finales y administradores del sistema.

B.4. Estrategia de Calidad

Para alcanzar los objetivos de calidad, se adoptarán las siguientes estrategias:

- **Revisión y Validación de Requisitos**: Verificar que todos los requisitos del proyecto estén claros, completos y sean factibles.
- **Pruebas Exhaustivas**: Realizar pruebas de instalación, configuración, integración y funcionalidad para asegurar que el sistema opere correctamente.
- **Auditorías de Seguridad**: Ejecutar auditorías para evaluar la seguridad del sistema y la conformidad con las políticas de seguridad de NTT Data.
- **Capacitación de Usuarios**: Asegurar que los usuarios finales y administradores reciban formación adecuada para utilizar y gestionar PAM360 eficientemente.

B.5. Procesos para Garantizar la Calidad

Revisión de Documentación

- **Documentación Técnica**: Revisión de manuales, guías de instalación y configuración proporcionados por ManageEngine.

Pruebas y Validaciones

- **Pruebas de Instalación**: Verificación de la correcta instalación de PAM360 en el entorno virtualizado.
- **Pruebas de Configuración**: Asegurar que todas las configuraciones necesarias (autenticación, políticas de seguridad, integración con AD) se realicen correctamente.
- **Pruebas Funcionales**: Validación de todas las funcionalidades de PAM360, incluyendo la gestión de usuarios, contraseñas y auditorías.

- **Pruebas de Seguridad**: Realizar pruebas de penetración y vulnerabilidad para identificar y mitigar posibles riesgos de seguridad.

Control de Cambios

- **Gestión de Cambios**: Implementar un sistema de control de cambios para manejar las modificaciones en los requisitos, el diseño o la configuración de PAM360.
- **Aprobación de Cambios**: Todos los cambios deben ser revisados y aprobados por el equipo de proyecto antes de su implementación.

B.6. Criterios de Aceptación

Los criterios para aceptar el proyecto incluyen:

- **Cumplimiento de Requisitos**: Todos los requisitos del proyecto deben ser cumplidos satisfactoriamente.
- **Validación de Funcionalidades**: Todas las funcionalidades de PAM360 deben operar sin errores y conforme a las especificaciones.
- **Resultados de Pruebas y Auditorías**: Los resultados de las pruebas y auditorías deben demostrar que el sistema es seguro y funcional.

B.7. Métricas de Calidad

Para medir la calidad del proyecto, se utilizarán las siguientes métricas:

- **Tasa de Éxito de Pruebas**: Porcentaje de pruebas que se completan exitosamente sin errores.
- **Número de Incidentes de Seguridad**: Cantidad de incidentes de seguridad detectados y corregidos durante el proyecto.
- **Satisfacción de Usuarios**: Nivel de satisfacción de los usuarios finales y administradores con el sistema implementado.
- **Tiempo de Respuesta a Incidentes**: Tiempo promedio para detectar y resolver incidentes o problemas en el sistema.

B.8. Responsabilidades

- **Gestor de Calidad**: Responsable de la planificación, ejecución y seguimiento de las actividades de aseguramiento y control de calidad.
- **Equipo de Proyecto**: Participar en las pruebas, auditorías y revisiones de calidad.

Apéndice C

Especificación de permisos

C.1. Roles Predefinidos en PAM360

PAM360 proporciona varios roles predefinidos, cada uno con un conjunto específico de permisos que determinan las acciones que los usuarios pueden o no pueden realizar dentro del sistema. Estos roles están diseñados para cubrir las necesidades seguridad de la plataforma y es uno de los principales sentidos de su uso. A continuación, se describen los roles y sus permisos:

Privileged Administrator (Administrador Privilegiado)

- **Descripción**: Este rol tiene privilegios similares a los de un administrador predeterminado, pero con capacidades adicionales para configurar la privacidad y los controles de seguridad.
- **Permisos**:
  - Manage Users (Gestionar Usuarios)
  - Manage Resources (Gestionar Recursos)
  - Manage Passwords (Gestionar Contraseñas)
  - View Passwords (Ver Contraseñas)
  - Managing Personal Passwords (Gestionar Contraseñas Personales)
  - View Audit and Reports (Ver Auditorías y Reportes)
  - Privacy and Security Controls (Controles de Privacidad y Seguridad)

- Remote Access, File Transfer, and Remote App Access (Acceso Remoto, Transferencia de Archivos y Acceso a Aplicaciones Remotas)

Administrator (Administrador)

- **Descripción**: Este rol permite la creación, configuración y administración de recursos y usuarios, así como la gestión de contraseñas y la visualización de auditorías y reportes.
- **Permisos**:
  - Manage Users
  - Manage Resources
  - Manage Passwords
  - View Passwords
  - Managing Personal Passwords
  - View Audit and Reports

Password Administrator (Administrador de Contraseñas)

- **Descripción**: El administrador de contraseñas tiene la capacidad de gestionar y visualizar todas las contraseñas en el sistema, excepto las contraseñas personales de otros usuarios.
- **Permisos**:
  - Manage Passwords
  - View Passwords
  - Managing Personal Passwords

Password Auditor (Auditor de Contraseñas)

- **Descripción**: Este rol está enfocado en la auditoría y revisión de las contraseñas sin la capacidad de realizar cambios.
- **Permisos**:
  - View Passwords
  - View Audit and Reports

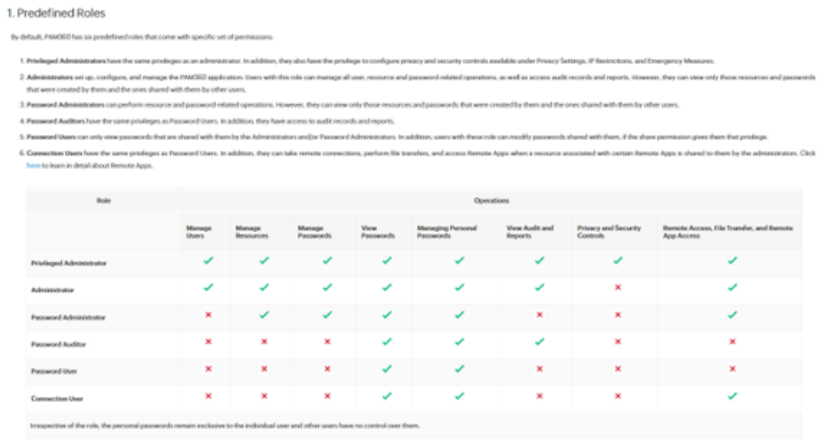
Password User (Usuario de Contraseñas)

- **Descripción**: Los usuarios con este rol pueden ver las contraseñas que se han compartido con ellos por los administradores.
- **Permisos**:
  - View Passwords
  - Managing Personal Passwords

Connection User (Usuario de Conexión)

- **Descripción**: Este rol permite a los usuarios tomar conexiones remotas y realizar transferencias de archivos.
- **Permisos**:
  - Remote Access, File Transfer, and Remote App Access

Resumen de Permisos por Rol



1. Predefined Roles

By default, PAM360 has six predefined roles that come with specific set of permissions:

1. **Privileged Administrators** have the same privileges as an administrator. In addition, they also have the privilege to configure privacy and security controls available under Privacy Settings, IP Restrictions, and Emergency Measures.
2. **Administrators** set up, configure, and manage the PAM360 application. Users with this role can manage all user, resource and password related operations, as well as access audit records and reports. However, they can view only those resources and passwords that were created by them and the ones shared with them by other users.
3. **Password Administrators** can perform resource and password related operations. However, they can view only those resources and passwords that were created by them and the ones shared with them by other users.
4. **Password Auditors** have the same privileges as Password Users. In addition, they have access to audit records and reports.
5. **Password Users** can only view passwords that are shared with them by the Administrators and/or Password Administrators. In addition, users with these role can modify passwords shared with them, if the share permission gives them that privilege.
6. **Connection Users** have the same privileges as Password Users. In addition, they can take remote connections, perform file transfers, and access Remote Apps when a resource associated with certain Remote Apps is shared to them by the administrators. Click here to learn in detail about Remote Apps.

Role	Operations							
	Manage Users	Manage Resources	Manage Passwords	View Passwords	Managing Personal Passwords	View Audit and Reports	Privacy and Security Controls	Remote Access, File Transfer, and Remote App Access
Privileged Administrator	✓	✓	✓	✓	✓	✓	✓	✓
Administrator	✓	✓	✓	✓	✓	✓	×	✓
Password Administrator	×	✓	✓	✓	✓	×	×	✓
Password Auditor	×	×	×	✓	✓	✓	×	×
Password User	×	×	×	✓	✓	×	×	×
Connection User	×	×	×	✓	✓	×	×	✓

Irrespective of the role, the personal passwords remain exclusive to the individual user and other users have no control over them.

Figura C.1: roles PAM360.