ADISTEC PROFESSIONAL SERVICES

Safeguard® Rapid Deploy for Privileged Password

DESCRIPCIÓN

Nuestro paquete de implementación ayuda a nuestros clientes en la implementación de One Identity Safeguard for Privileged Password para la administración de accesos privilegiado a credenciales (contraseñas y/o claves). Este paquete está diseñado tanto para clientes con requerimientos básicos como así para empresas con una política ya definida de protección y administración de acceso.

ALCANCES DE NUESTRO SERVICIO

- → Assessment
  - Kick Off.
  - Workshop de Descubrimiento.
    - Definición de factores de éxito, hasta dos (2) casos de uso.
    - Análisis de la infraestructura actual.
      - Relevamiento de domino y forest de AD.
      - Determinar usuarios y grupos funcionales.
    - Relevamiento de flujo de liberación de credenciales privilegiadas.
  - Presentación del informe.
- → Diseño
  - Análisis escenario y condiciones.
  - Arquitectura
    - Stand Alone
      - Hasta un (01) Appliance físico o virtual.
      - Configuración de parámetros de networking.
    - Alta Disponibilidad
      - Hasta tres (03) Appliance físico o virtual.
      - Configuración de parámetros de networking.
  - Diseño Alto Nivel (HLD)
    - Diseño de alto nivel a partir de los resultados del taller
      - Puertos.
      - Nombre de máquinas.
      - Redes.
      - Interacción con Firewall & Antivirus.
  - Diseño bajo nivel (LLD)
    - Diseño de bajo nivel a partir de los resultados del taller
      - Configuración del dominio.
      - Definir grupos de cuentas privilegiadas.
      - Creación de hasta un (01) grupo nuevo o supervisión de hasta tres (03) grupos actuales.
      - Diseño de flujo de gestión de credenciales
        - Definición de hasta dos (02) reglas.
        - Definición de hasta dos (02) políticas.
  - Diseño del Disaster Recovery Plan (DRP).
  - Presentación de HLD y LLD.

ALCANCES DE NUESTRO SERVICIO (continuación)

→ Desarrollo
- Instalación de hasta un (01) entorno de Desarrollo
  - Instalar dispositivos (Safeguard) en el entorno Desarrollo o Prueba.
  - Configuración básica de PAM.
  - Integración con el repositorio de usuarios
    - Hasta un (01) Active Directory (perteneciente a un [01] Forest).
  - Integración con sistemas o dispositivos
    - Hasta un (01) sistema Windows.
    - Hasta un (01) Linux.
    - Establecer la configuración de PPM contra la política de permisos.
  - Integración un (01) dispositivos de red al sistema PAM (*opcional*)
    - Prueba de uso de protocolo Telnet o SSH.
    - Establecer la configuración de PPM contra la política de permisos.
  - Creación de Guía de instalación.
  - Testing
    - Pruebas de aceptación, 2 casos de uso definidos en etapa Assessment.

→ Implementación
- Instalación de PAM en un (01) entorno de Producción.
  - Pasar a producción los dispositivos Safeguard.
  - Importar configuración desde entorno Desarrollo o Prueba.
  - Integración con hasta veinte (20) sistemas
    - Dispositivos compatibles con acceso Telnet o SSH.
    - Computadoras con Sistemas Operativo Microsoft Windows o Linux.
  - Configuración global
    - Alta Disponibilidad (*según arquitectura*).
    - Recuperación ante desastres (*según arquitectura*).

→ Testing y QA
- Pruebas de 2 casos de uso definidos en etapa Assessment.
- Proceso de solicitud de cuenta de administración
  - Hasta un (01) sistema con Microsoft Windows.
  - Hasta un (01) sistema con Linux.
  - Hasta un (01) dispositivo a través de Telnet o SSH.
- Test de aceptación
- Skill Transfer
  - Modalidad Remota.
  - Hasta (04) cuatro asistentes.
  - Duración: 6 horas.

DETALLES DEL SERVICIO

Modalidad: On-Line
Duración Estimada: 160 horas

PART NUMBER

P/N	Descripción
APS-QST-SFGPPRD	Safeguard® Rapid Deploy for Privileged Password

LIMITACIONES Y FUERA DE ALCANCE

No está incluido en este servicio la instalación física de el/los appliance/s, el cliente debe realizar el rack & stack de/los appliance/s. Para appliances virtuales, el proceso de importación debe ser ejecutado por el cliente. Queda fuera del alcance la configuración de networking (ya sea físico o virtual) y network load balancer para la correcta operatividad de los appliances. Adistec no asegura ni garantiza la compatibilidad de los dispositivos, sistemas o aplicaciones que no estén en el listado público de plataforma homologados por Quest (Aquí).Si el sistema, aplicación o dispositivo no estuviera en la lista de compatibilidad de Quest, Adistec se compromete a realizar todos los esfuerzos comercialmente razonables (siempre y cuando no pongan el riesgo el plan de trabajo y los plazos programados) para trabajar en un workaround que permita su integración, pero sin asegurar o garantizar la misma. Se define un Sistema como una aplicación, un sistema operativo, una base de datos o un dispositivo de red compatible según la matriz de compatibilidad de la solución, que cuenten con una estructura de administración de cuentas única para ser administrado por el Software