

ADISTEC PROFESSIONAL SERVICES

Rapid Deploy for One Identity® Safeguard

DESCRIÇÃO

Nosso pacote de implementação auxilia nossos clientes na implantação do One Identity Safeguard para o gerenciamento de acesso privilegiado a credenciais (senhas e/ou chaves). Este pacote é projetado tanto para clientes com requisitos avançados quanto para empresas com uma política já definida de gestão de proteção e acesso.

ESCOPO DO NOSSO SERVIÇO

- Avaliação
 - Kick off.
 - Workshop de descobrimento.
 - Definição de fatores de êxito, até dois (2) casos de uso.
 - Análise da infraestrutura atual.
 - Levantamento de domínios e florestas do AD.
 - Levantamento de usuários e grupos funcionais.
 - Levantamento do fluxo de liberação de credenciais privilegiadas.
 - Apresentação dos relatórios.
 - Descobertas.
 - Recomendações e opções de implantação de práticas recomendadas.
- Design
 - Análise de cenários e condições
 - Arquitetura:
 - Stand Alone
 - Até um (01) Appliance físico ou virtual para gerenciamento de credenciais (senhas e/ou chaves).
 - Até um (01) Appliance físico ou virtual para gravação de sessão e análise comportamental.
 - Configuração dos parâmetros de rede.
 - High Availability
 - Até três (03) Appliances físicos ou virtuais para gerenciamento de credenciais (senhas e/ou chaves).
 - Até dois (02) Appliances físicos ou virtuais para gravação de sessão e análise comportamental.
 - Configuração dos parâmetros de rede.
 - Design de alto nível (HLD)
 - Design de alto nível com base nos resultados do workshop
 - Portas.
 - Nome das máquinas.
 - Redes.
 - Interação com Firewall & Antivírus.

ESCOPO DO NOSSO SERVIÇO (continuação)

- Design de baixo nível (LLD)
 - Design de baixo nível com base nos resultados do workshop
 - Configuração do domínio
 - Definição de grupos de contas privilegiadas
 - Criação de até um (01) novo grupo ou monitoração de até três (03) grupos atuais
 - Design do fluxo de gerenciamento de credenciais
 - Definição de até duas (02) regras
 - Definição de até duas (02) políticas
- Design do Plano de Recuperação de Desastres (DRP)
- Apresentação dos HLD e LLD

→ Desenvolvimento

- Instalação de até um (01) ambiente de desenvolvimento ou teste.
 - Instalação do dispositivo (One Identity Safeguard) no ambiente de desenvolvimento ou teste.
 - Configuração básica do PAM (Privileged Access Management).
 - Integração com o repositório de usuários
 - Até um (01) Active Directory (pertencente a uma [01] Floresta).
 - Integração com sistemas ou dispositivos
 - Até um (01) sistema Windows.
 - Até um (01) Linux.
 - Estabelecimento das configurações do PPM em relação à política de permissões.
 - Estabelecimento das configurações de PPM (Privileged Passwords Management) em relação à política de permissões.
 - Estabelecimento das configurações de PSM (Privileged Sessions Management) em relação à política de permissões.
 - Integração de um (01) dispositivo de rede no sistema Privileged Access Management (PAM *opcional*).
 - Testes utilizando o protocolo Telnet ou SSH
 - Estabelecimento das configurações de PPM (Privileged Passwords Management) em relação à política de permissões.
 - Estabelecimento das configurações de Privileged Sessions Management (PSM) em relação à política de permissões
 - Criação do Guia de Instalação.
 - Testing
 - Provas de aceitação, até dois (2) casos de uso.

ESCOPO DO NOSSO SERVIÇO (continuação)

- Implementação
 - Instalação de PAM em um (01) Ambiente de produção.
 - Movimentação à produção dos dispositivos de Safeguard.
 - Configurações de importação do ambiente de desenvolvimento ou teste.
 - Integração com até vinte (20) sistemas.
 - Dispositivos compatíveis com acesso Telnet ou SSH
 - Sistemas com Microsoft Windows ou Linux
 - Configurações globais
 - Alta Disponibilidade (*de acordo com a arquitetura*)
 - Plano de recuperação de desastres (*de acordo com a arquitetura*)

- Testing e QA
 - Testes, até dois (2) casos de uso .
 - Processo de solicitação de conta de administrador
 - Até um (01) sistema com Microsoft Windows.
 - Até um (01) sistema Linux.
 - Até um (01) dispositivo via Telnet ou SSH.
 - Testes de aceitação.
 - Transferência de habilidades
 - Modo Remoto.
 - Até (04) quatro participantes.
 - Duração: 6 horas

DETALHES DO SERVIÇO

Modalidade: On-Line

Duração Estimada: 220 horas

PART NUMBER

P/N	Descrição
APS-QST-OISFRD	Rapid Deploy for One Identity Safeguard®

LIMITAÇÕES E FORA DE ALCANCE

A instalação física do aparelho não está incluída neste serviço, o próprio cliente deve realizar o rack & stack do(s) appliance(s). Para appliances virtuais, o processo de importação deve ser executado pelo cliente. Está fora do escopo a configuração de rede (física ou virtual) e de Load Balancers para o correto funcionamento dos appliances. A Adistec não assegura nem garante a compatibilidade de dispositivos, sistemas ou aplicativos que não estejam na lista pública de plataformas aprovadas pela Quest ([Aqui](#)). Se o sistema, aplicativo ou dispositivo não estiver na lista de compatibilidade da Quest, a Adistec se compromete a fazer todos os esforços comercialmente razoáveis (desde que não coloquem em risco o plano de trabalho e os prazos programados) para trabalhar em uma solução alternativa que permita sua integração, mas sem assegurar ou garantir a mesma. Um sistema é definido como um aplicativo, sistema operacional, banco de dados ou dispositivo de rede compatível, com base na matriz de compatibilidade da solução, que contenha uma estrutura única de administração de contas a ser gerenciada pelo Software.