SONDA®
make it easy

DESCRITIVO COFRE DE SENHAS

ÍNDICE

1. Versão do Produto

Versão	Escopo	Data de Atualização
Versão 01	Criação do documento	-

2. Descrição Resumida

Senhas corporativas são as chaves para o coração da empresa e as pessoas que as possuem podem ter acesso total e irrestrito sobre os sistemas e dados, o que aumentará exponencialmente o risco de segurança sobre esses ativos.

A má gestão das credenciais privilegiadas (admins e superusuários) é considerada uma brecha enorme na segurança da informação corporativa atual. Essas credenciais, por muitas vezes, são compartilhadas entre diversos profissionais o que impossibilita, na maioria dos casos, a identificação do responsável pela operação realizada.

A gestão das credencias privilegiadas tornou-se uma atividade complexa e necessária para a maioria das organizações. Visando auxiliar os **CLIENTES** nessa atividade, a **SONDA** oferece o serviço Cofre de Senha.

O Cofre de Senha **SONDA** é um repositório seguro de forte proteção e criptografia que guardam as senhas corporativas de administração do ambiente tecnológico, onde somente pessoas autorizadas têm credenciais de acesso.

Por meio dessa solução é possível o acompanhamento rigoroso de quem usou ou está utilizando, quais as atividades realizadas e onde foram realizadas. Os logs e relatórios garantem uma gestão mais ampla protegendo a TI em casos extremos. Desta forma, é possível permitir aos profissionais de TI terem acesso ao parque de servidores e dispositivos de rede exclusivamente através do cofre, diminuindo o número de usuários com privilégios administrativos e permitindo a rastreabilidade das ações executadas pelos analistas.

3. Objetivo

O objetivo de um cofre de senhas é fornecer um local seguro para armazenar e gerenciar senhas de forma criptografada, oferecendo acesso protegido por uma senha mestra ou autenticação adicional. Ele facilita a organização e proteção das credenciais, promovendo a segurança online ao evitar o uso de senhas fracas e repetidas, além de simplificar o processo de login, garantindo o acesso seguro a várias contas e serviços digitais.

4. Benefícios

Um cofre de senhas oferece uma série de benefícios importantes para os **CLIENTES**:

- **Segurança Avançada:** Um cofre de senhas usa técnicas de criptografia para manter as senhas seguras contra acesso não autorizado;
- **Senhas Fortes:** Ajuda a criar senhas complexas e únicas para diferentes contas, aumentando a segurança online;
- **Evita Senhas Repetidas:** Previne o uso da mesma senha em várias contas, reduzindo o risco de violações de segurança em cascata;
- **Facilita a Gestão:** Permite armazenar todas as senhas em um local centralizado, facilitando a gestão e organização das credenciais;

- **Acesso Simples:** Oferece acesso fácil e seguro às senhas quando necessário, geralmente com uma única senha mestra ou autenticação biométrica;
- **Compartilhamento Seguro:** Facilita o compartilhamento seguro de senhas com pessoas de confiança, como familiares ou colegas de trabalho;
- **Registro Seguro de Informações:** Além de senhas, muitos cofres de senhas também permitem armazenar outras informações confidenciais, como números de cartões de crédito e notas seguras;
- **Proteção Contra Phishing:** Reduz o risco de phishing, pois os usuários não precisam digitar manualmente as senhas em sites, minimizando a exposição a ataques de phishing;
- **Alertas de Segurança:** Alguns cofres de senhas oferecem recursos de alerta que notificam os usuários sobre senhas fracas ou comprometidas;
- **Conformidade e Auditoria:** Em ambientes corporativos, ajuda a manter a conformidade com políticas de segurança e permite auditoria das atividades relacionadas às senhas;
- **Recuperação de Conta**: Facilita a recuperação de contas em caso de esquecimento de senhas, evitando o problema de ser bloqueado devido a senhas perdidas;
- **Economia de Tempo:** Agiliza o processo de login, economizando tempo ao preencher automaticamente informações de login em sites e aplicativos;

5. Escopo de Atuação

Credenciais de qualquer tipo, sejam elas senhas ou padrões de acesso, são, em teoria, uma informação intransponível e completamente pessoal. Mas, não é exatamente isso que acontece na prática do dia a dia empresarial. Muitas vezes, em uma equipe cujas tarefas sejam de responsabilidade de diversos membros, por exemplo, as senhas são compartilhadas entre si para que todos tenham como cumprir com suas funções. O que é perfeitamente necessário, porém, não deixa de trazer um risco no pacote. Logo, uma conta privilegiada se torna ao alcance de várias pessoas e, em caso de um deslize de conduta, fica difícil atribuir a autoria dos atos que foram prejudiciais a toda credibilidade da empresa.

Buscando evitar esse tipo de situação o Cofre de Senha **SONDA** assegura que as senhas de alto privilégio sejam guardadas e controladas através de processo e tecnologia segura.

6. Ofertas

Com o Cofre de Senha **SONDA**, mesmo que o acesso seja realizado através de uma conta administrativa genérica e de conhecimento de todos os funcionários, informações como horário de acesso, servidor utilizado e, até mesmo, quantas e quais foram suas interações com o sistema, seja via mouse ou teclado, são retidas são armazenadas com total precisão e segurança.

Caso seja necessário a visualização da senha, a solução permite adicionar controle de dupla custódia, para que mais de uma pessoa precise fornecer partes da senha, ou ainda através de workflow de aprovação, permitindo que gestores autorizem antes que o cofre forneça a informação.

A solução Cofre de Senha **SONDA** é dividido da seguinte forma:

- **Agente Usuário (obrigatório):** módulo principal da solução, onde são contabilizados o número de usuários que terão acesso a console padrão da solução;
- **Agente Servidor:** troca de senhas de servidores. Para cada servidor que houver o gerenciamento de credenciais é necessária uma licença deste módulo (unidade do vendável: servidor);
- **Agente de Banco de Dados:** permite a troca de senhas na camada de banco de dados, tais como Oracle, SQL Server e My SQL. Para cada instância de banco que houver o gerenciamento de credenciais é necessária uma licença deste módulo (unidade do vendável: instância);

- **Agente Redes:** troca de Dispositivos de Rede, tais como Firewall, roteadores e switches. Para cada dispositivo de rede que houver o gerenciamento de credenciais é necessária uma licença deste módulo (unidade do vendável: dispositivos de rede).

Nota: é obrigatório a inclusão de pelo menos uma licença do Agende Usuário, ou seja, não é permitido a venda das licenças dos demais.

A oferta do Cofre de Senha pode ser entregue de três formas:

- Gestão **SONDA**;
- Compartilhada;
- Gestão **CLIENTE** com suporte **SONDA** (Neste caso, é necessário criar a infraestrutura da solução dedicada para o **CLIENTE)**.

6.1. Entregáveis

Será entregue, mensalmente, ao **CLIENTE** um relatório de rastreabilidade o qual contemplará todas as ações executas pelos profissionais que tiveram acesso do servidor por meio da solução Cofre de Senha. Solicitações esporádicas do **CLIENTE** deverão ser atendidas pelo processo de requisições da **SONDA**.

6.2. Requisitos técnicos não funcionais

- Gerenciamento e utilização da solução através de interface Web;
- Compatibilidade com navegadores Google Chrome, Firefox, Internet Explorer e outros;
- Possibilidade de segregação de funções, baseado em perfis de acesso;
- Permite login dos usuários da solução utilizando dois fatores de autenticação;
- Possibilidade de dois ou mais usuários solicitarem acesso a mesma conta privilegiada e/ou genérica, sem comprometimento da rastreabilidade;
- Permite aos administradores se autenticarem na interface de gerência da solução através de certificado digital;
- Discovery de Certificados em sites, servidores de aplicação e diretórios de rede. Armazena de forma segura, controla os responsáveis e a data de vencimento, oferecendo a opção de alerta ou renovação automática, através de API de integração de mercado.
- A requisição de um Certificado Digital pode ser realizada, auto assinada e publicada diretamente na solução;
- Gestão automatizada de todo ciclo de vida de um Certificados Digital;
- A interface Web que suporta a utilização de certificados digitais válidos pela ICP-Brasil e certificados auto assinados gerados pela própria solução;
- Opera como proxy de conexões via SSH/TELNET para qualquer dispositivo gerenciado, através de **CLIENTE**S SSH como PuTTy, MobaXTerm, secureCRT e outros, sem a necessidade de abertura de um Terminal Service;
- Prove conexões RDP controladas;
- Autentica de forma confiável todas as requisições de senhas realizadas pela solução, com a finalidade de não permitir que qualquer usuário ou código malicioso tenha acesso ao repositório de senhas;
- Todas as transmissões de dados entre os componentes da solução são criptografadas;
- Sobre a utilização de padrões criptográficos por determinadas funcionalidades, a solução atende aos seguintes requisitos:
    - Utiliza algoritmo AES-256 para criptografia do tráfego de informações;

  - Para operações de autenticação e de acordo de chave de sessão, permite a utilização de algoritmos dos sistemas de criptografia de chave pública RSA, Google Authenticator ou ECC;
  - Permite a utilização de chaves para os algoritmos do sistema de criptografia ECC;
  - Permite a utilização de chaves de curvas Brainpool (RFC 5639) para os algoritmos do sistema de criptografia ECC;
  - Permite a utilização de chaves para os algoritmos do sistema de criptografia RSA;
  - Compatível com os seguintes sistemas/aplicações COF;
  - Sistemas Operacionais: Windows Server 2008 e superiores, Red Hat Enterprise Linux 6 ou superiores e AIX 61. E 7.1;
  - Aplicações Windows: Contas de serviço englobando contas de serviço do SQL server em cluster, tarefas agendadas, pools de conexão do IIS, COM+, usuário anônimo do IIS, serviços de Cluster;
  - Sistemas Gerenciadores de Banco de Dados: Oracle, Oracle RAC, MSSQL, MySQL;
  - Appliances de Segurança: CheckPoint, Nokia, Cisco, IBM, SourceFire e Imperva;
  - Dispositivos de redes: Cisco, D-Link, HP, 3com, Alcatel, Foundry, Brocade e ARUBA;
  - Middleware: WebLogic, JBOSS, Tomcat, Peoplesoft, Oracle Application Server, Apache e IIS;
  - Serviços de Diretórios: OpenLDAP;
  - Acesso Remoto e monitoração: CA, IBM (Incluindo a HMC – Hardware Management Console dos servidores IBM), HP, iLO, Sun, Dell, DRAC, Digi, Cyclades, Fujitsu;
  - Ambientes Virtuais: VMware e Openstack;
  - Storages: Hitachi, EMC e IBM;
- Possui integração com Hardware Security Management (HSM) para aumentar a segurança física;
- Integração nativa com soluções de SIEM/Syslog;
- Possibilidade de integração com ferramentas de Gestão de Mudanças;
- Possui workflow de aprovação para uso de credenciais;
- Flexibilidade no processo de aprovação para o acesso a contas privilegiadas (acessos pré-aprovados, acessos com aprovação única, acessos com aprovação dupla ou outros que possam compor a solução)
- Armazenamento e consulta de logs que forneçam as seguintes informações:
  - Identificação do usuário que realizou determinado acesso a um dispositivo;
  - Identificação de quem aprovou o acesso do usuário;
  - Data e hora do acesso realizado e das ações que o usuário realizou no dispositivo remoto;
  - Filtros para a recuperação de logs;
  - Usuário;
  - Sistema-alvo acessado;
  - Tipo de atividade;
  - Intervalo de tempo (data/hora/minuto inicial e final).
- Vem acompanhado de todas as licenças de software ou hardware necessárias para atendimento das funcionalidades da solução;
- Disponibiliza os modelos de troca de senha de forma que podem ser abertos, editados e auditados;
- Não depende de sistema operacional externo e/ou banco de dados que geram a necessidade de licenças adicionais de outros fabricantes;
- Não possui necessidade de utilização de ferramentas de terceiros para completar a solução, ou seja, um fabricante único que atende todas as necessidades de um Cofre de Senhas;
- Possibilidade de configuração em cluster de contingência, alta disponibilidade (HA) ou recuperação de desastres (DR);
- Possibilidade de configuração do backup da solução e seus dados conforme Política de Backup da empresa;
- Interface em Português do Brasil;

- Aderente às Normas ISO/ IEC 27.001, SOX e PCI.

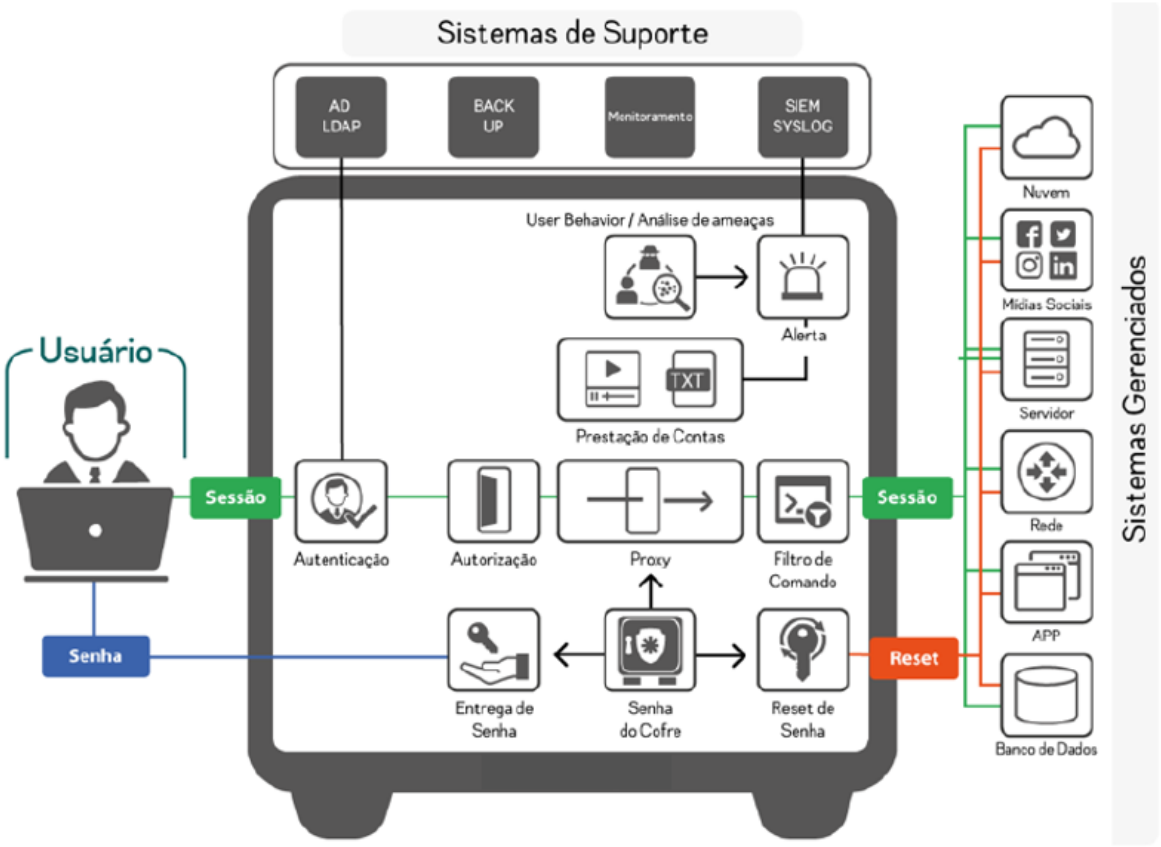
6.3. Requisitos técnicos funcionais

- Gerenciamento de todo o ambiente sem a necessidade de instalação de agentes ou qualquer software nos sistemas-alvos ou dispositivos de rede;
- Geração automática de senhas de alta complexidade de acordo com as regras de cada tecnologia e Política de Segurança da empresa;
- Realiza a troca automática das senhas, em horário programado, após terem sido liberadas para uso ou por vencimento de prazo;
- Possibilidade de gerenciar senhas privilegiadas em aplicações e integração com sistemas legado;
- Oferece interface com visão personalizada exclusiva para Auditorias e Órgãos Reguladores;
- Provê área de transferência segura, de forma que o solicitante possa visualizar a senha ou copiá-la para a tela de login do sistema-alvo;
- Liberação ou revogação de todos os acessos de uma determinada credencial de maneira automatizada e imediata;
- Provisionamento de usuários locais em servidores Linux/Unix, Windows ou dispositivos de rede;
- Notifica, via e-mail ou SMS, novas solicitações de aprovação de acesso aos respectivos responsáveis pelas credenciais;
- Permite o monitoramento on-line do uso das contas e desligamento da sessão;
- Possui o recurso "break glass" para acesso de emergência às contas, ou seja, permitirá acesso a ativos protegidos de forma emergencial, sem a necessidade de aprovação prévia em contas no qual o usuário não teria acesso, sem perda de rastreabilidade (como esse recurso é habilitado);
- Oferece a funcionalidade de "Discovery" para realizar busca de novos servidores e elementos de rede, sendo capaz de levantar automaticamente as contas criadas nesses novos dispositivos;
- Possibilidade de bloqueio e auditoria de comandos específicos;
- Busca por comandos específicos executados pelo usuário através de linha de comando logs ou sessões gravadas;
- Configuração de alertas imediatos quando realizados determinados comandos por usuários privilegiado;
- Possibilidade de geração de relatórios baseados nos logs e exporta para arquivos em formato ".csv";
- Extrair informações do servidor localizado nos Data Centers remotos caso seja necessário restaurar todas as configurações e os dados da solução de cofre de senhas;
- Possui mecanismo para exportar arquivo com as últimas senhas para repositório remoto, de forma criptografada e protegida por senha de múltipla custódia para recuperações de senhas no caso de falha total da solução;
- Possibilidade de arquitetura Ativo/Ativo sem a necessidade de um cluster externo à solução;
- No caso de falha de um dos servidores do cluster de cofre de senhas de alta disponibilidade local, cada um dos servidores deve tratar todas as requisições de acesso, sem nenhum prejuízo no desempenho ou nas funcionalidades;
- Alterações realizadas no cluster de cofre de senhas de alta disponibilidade local devem ser automaticamente replicadas para os outros servidores de redundância, de forma assíncrona e com delay máximo de 50ms;
- Utiliza tecnologia de restrição e autenticação que inclui Assinatura Digital (Hash), Path e endereço IP do host ou conjunto de hosts a serem acessados pela solução;
- Possibilidade de comunicação com os serviços de diretório via protocolo LDAPS;
- Possibilidade de implementação SNMP sobre IPv6;
- Implementa a especificação IETF RFC 2460, referente ao protocolo IPv6;

- Possibilidade de implementar a MIB II, conforme RFC 1213;
- Suportar sincronização do relógio interno via protocolo NTP e atualização automática do horário de verão com suporte e customização local;
- Acesso transparece permite que o usuário realize acesso aos dispositivos sem que seja exibida a senha ao usuário solicitante.

6.4. Ferramenta

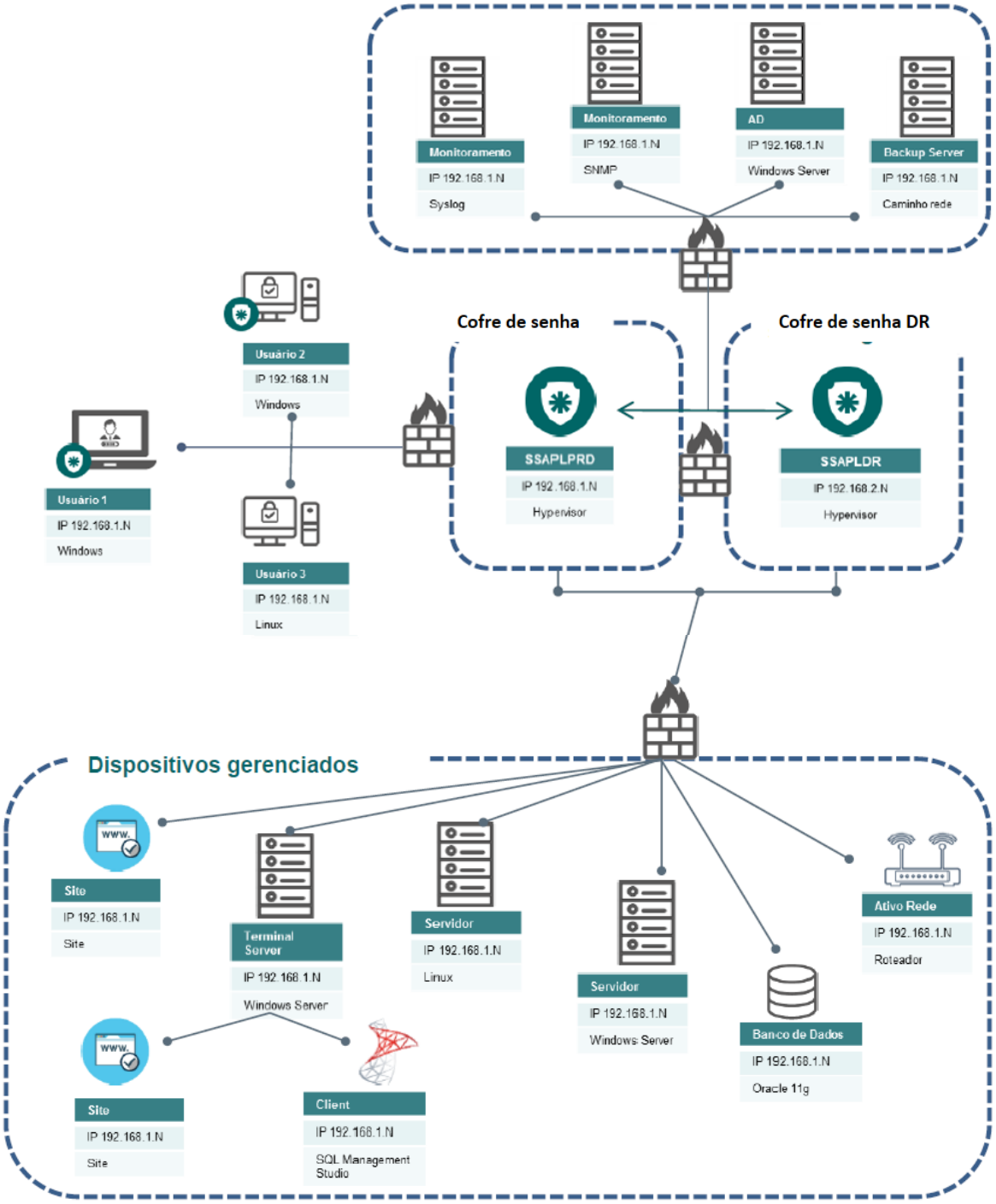
A solução consiste em gerenciar e alterar, por uso ou por expiração, as credenciais impessoais e/ou de alto privilégio nos ativos de rede, servidores, bancos de dados e aplicações. Segue abaixo um diagrama para ilustrar a abrangência da solução.



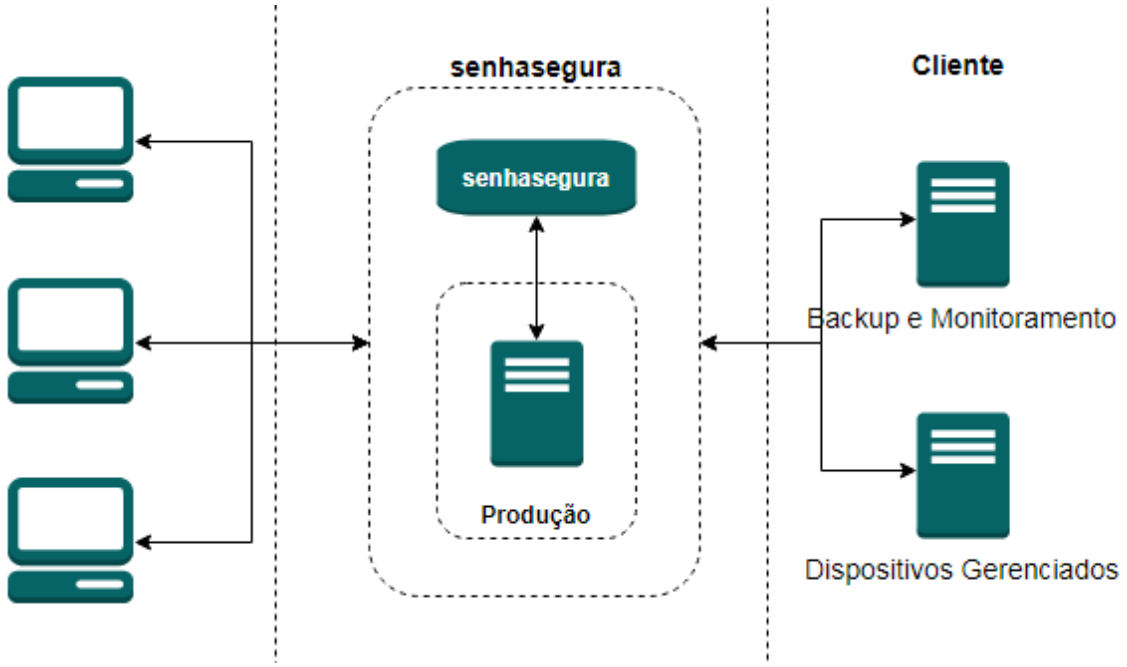
6.5. Desenho da Solução

6.5.1. Topologia de exemplo

Topologia geral e arquitetura do ambiente de Cofre de Senha **SONDA**.



6.5.2. Arquitetura



7. Premissas e Requisitos

- Banco de dados próprio sem necessidade de licenças;
- Interface Web embarcada, sem necessidades de licenças ou recursos adicionais;
- Nos appliances, apenas as portas de serviços estão liberadas:

Protocolo/Porta	Função
TCP/22	SSH Server
TCP/80	Web Server com redirecionamento para porta 443
TCP/443	Server da aplicação Web
UDP/161 UDP/162	SNMP
TCP/3389	RDP Proxy
TCP/3306 TCP/4444 TCP/4567 TCP/4568 UDP/4567	Cluster de Base de Dados

- Com base nos equipamentos identificados através do módulo scan e discovery o **CLIENTE** deverá indicar quais equipamentos serão importados para Solução;
- Configuração dos usuários do Active Directory (AD) e perfis associados aos grupos de atuação na solução;
- O **CLIENTE** deverá indicar quais credenciais poderão ser habilitadas para troca de senhas;
- Não faz parte do escopo da solução qualquer configuração em equipamentos ou aplicativos por parte da **SONDA**.
- **CLIENTES** no qual o ambiente esteja externo ao Data Center fará uso de VPN para acesso ao cofre;
- A integração com o Oracle Grid não faz parte deste escopo de implantação, se solicitada pela será tratada separadamente como Professional Services;

- Cofres de senha não tem função de controle, eles não evitam a execução de uma ação uma vez que o usuário tem a credencial liberada;
- Licença de Remote Desktop Services (RDS) - O Cofre de Senha necessita da funcionalidade RemoteApp do Windows Server, para abrir apenas um programa específico, como SQL Management Studio, Oracle Developer ou VSphere. Para utilizar essa funcionalidade, é necessário possuir um servidor (8VCPU e 4 VGB com 60 disco) com o RemoteApp habilitado. Assim, o custo da licença e do servidor devem ser calculados separadamente;
- Para certificados auto assinados, os arquivos .crt e .key deverão ser enviados ao time de segurança da **SONDA** para instalação no cofre de senha;
- Para a utilização das funções de notificação de eventos, workflows de aprovação, dados de utilização e robôs, devem ser fornecidas informações relativas aos servidores SMTP e IMAP/POP3.

8. Matriz de Responsabilidade

Para um melhor entendimento a matriz de responsabilidade será classificada com base na metodologia RASICO, onde: **R** - Responsável; **A** - Aprovador; **S** - solicita; **I** – Informado; **C** – Consulta e **O** - Opcional.

Descrição das Atividades	SONDA	CLIENTE	Ambos
Definição de Responsáveis em caso de quebras de senhas		R	
Configuração de toda solução	R		
Definição de Política de Retenção de Logs de Gravação			R
Definição de Grupos de Acesso ao Cofre		R	
Definição de Políticas de Senhas		R	
Definição de Formas de Acesso			R
Definição de Dispositivos a serem Importados		R	
Definição de Usuários a serem importados		R	
Configuração de Varredura de Dispositivos	R		
Importação de Dispositivos e Usuários	R		
Configuração de Grupos de Servidores x Acesso			R
Tombamento de senhas	R		
Configurar envio de alertas imediatos quando realizados determinados comandos por usuários privilegiado	R		
Automação da concessão ou revogação de acesso	R		
Backup das últimas senhas para repositório remoto	R		
Relatório de Auditorias	R		
Hardening do Ambiente	R		
Monitoramento de Sistema Operacional	R		
Monitoramento de Banco de Dados	R		

9. Requisições de Serviços

A tabela abaixo lista as requisições de serviços disponíveis para solicitações dos **CLIENTES** assim como seu tempo de solução e horário de cobertura.

Requisição	Classificação	Tempo de Solução
Configurar Grupo de Acesso ao Cofre de Senhas	E	Conforme TS contratado
Configurar Sincronização com Active Directory	E	Conforme TS contratado
Configurar Grupo de acesso de Servidores	E	Conforme TS contratado

Configurar Descoberta de Dispositivos	E	Conforme TS contratado
Configurar Descoberta de Credenciais	E	Conforme TS contratado
Importar Usuário	E	Conforme TS contratado
Importar Servidor	E	Conforme TS contratado
Fornecer gravação/log de Acesso	F	Conforme TS contratado
Gerar Vídeo/Log de Acessos	F	Conforme TS contratado
Gerar Relatórios de Auditoria	F	Conforme TS contratado
Atualização da Solução	C	Gestão de Mudança
Break Glass de Senhas	A	Conforme TS contratado
Recuperação de Ambiente	A	Conforme TS contratado

10.Níveis de Serviço

Serviço	Nome	Descrição	Meta
Cofre de senha	Disponibilidade do SIEM/Portal	Percentual de tempo que o serviço estará disponível, incluindo acessibilidade e funcionalidade, excluindo desse tempo as atividades de paralisação programada e demais exceções mencionadas em contrato.	99,86%


SONDA
make it easy