SONDA®
make it easy

DESCRITIVO SONDA HYBRID

ÍNDICE

1. Versão do Produto

Versão	Escopo	Data de Atualização
Versão 01	Criação do documento	-
Versão 02	Revisão e reformulação geral das ofertas	12/03/2025
Versão 03	Revisão e reformulação geral das ofertas	28/08/2025
Versão 04	Inclusão dos pré-requisitos de integração com as subscrições do CLIENTE e ambiente on-premise.	23/10/2025

2. Descrição Resumida

O **SONDA** Hybrid fornece uma solução de gerenciamento de nuvem e automação que unifica ambientes heterogêneos, incluindo nuvens públicas, privadas e híbridas. Com uma abordagem centrada na automação e na simplificação das operações, a plataforma capacita as equipes de TI a provisionar, gerenciar e otimizar recursos de maneira eficiente, reduzindo custos e aumentando a agilidade.

Com uma ampla gama de recursos e funcionalidades, o **SONDA** Hybrid permite o gerenciamento e provisionamento de recursos de forma eficiente, automação de fluxos de trabalho complexos e segurança em toda a infraestrutura de TI.

O **SONDA** Hybrid é destinado a toda empresa de médio ou grande porte cujas necessidades de TI envolvam a gestão de cargas de trabalho em múltiplas nuvens, sejam públicas ou privadas e que necessitem otimizar sua operação.

3. Objetivo

O **SONDA** Hybrid tem como objetivos:

- Simplificar e facilitar o uso de múltiplas plataformas de cloud do **CLIENTE**;
- Manter o controle e a capacidade administrativa de mais de uma nuvem;
- Melhorar a tomada de decisões com informações essenciais das plataformas de nuvem, incluindo sua estrutura de custos para maior otimização;
- Alinhar as capacidades de cada uma das plataformas cloud com as necessidades do negócio;
- Fortalecer a segurança na implementação e operação das diferentes plataformas cloud.

4. Benefícios

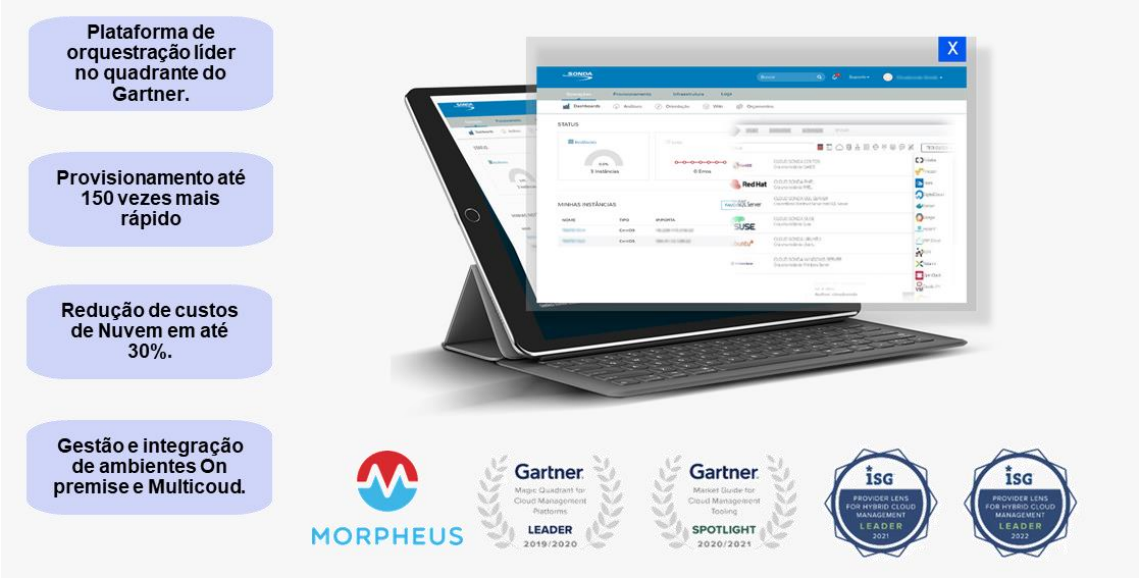
Os benefícios do **SONDA** Hybrid são:

- **Agilidade Operacional:** Reduz o tempo gasto em tarefas manuais e repetitivas, liberando equipes de TI para se concentrarem em atividades de maior valor;

- **Redução de Custos:** Otimiza o uso de recursos e minimiza gastos desnecessários com uma visão unificada de toda a infraestrutura;
- **Confiabilidade e Escalabilidade:** Garante a disponibilidade e a escalabilidade das aplicações, proporcionando uma experiência consistente para os usuários finais;
- **Segurança Reforçada:** Possibilita a implementação de controles de segurança em toda a infraestrutura e aplicação de políticas de conformidade para mitigar riscos;
- **Time to Market:** Maior agilidade na implementação de novas soluções e na gestão recorrente dos serviços (menor time-to-market, capacidade de experimentação);
- **Gestão:** Dispõe de visões analíticas e modelos preditivos para ajustar orçamentos às capacidades financeiras do negócio;
- **Flexibilidade:** Maior flexibilidade e eficiência ao estender as cargas de trabalho com processos mais adequados aos negócios.
- O **SONDA** Hybrid oferece um modelo de assinatura flexível, adaptado às necessidades específicas de cada **CLIENTE**.
- Processos certificados que garantem a qualidade e eficiência do serviço entregue;
- Otimização de processos e recursos, para que os serviços do **CLIENTE** fortaleçam a continuidade operacional com o melhor custo;
- Alianças estratégicas com os maiores agentes e provedores de Cloud do mercado;

5. Escopo de Atuação

O **SONDA** Hybrid utiliza tecnologias reconhecidas no mercado, com uma solução de gestão capaz de orquestrar a maior gama de tecnologias a partir de um ponto central, desenvolvendo integrações e criando visões únicas. Automatizamos e orquestramos os processos de governança e gestão do ambiente, possibilitando ao **CLIENTE**, por meio do portal, visualizar e interagir com seus ambientes contratados em diferentes provedores de cloud.



O **SONDA** Hybrid pode ser integrado com ferramentas ou sistemas financeiros do **CLIENTE**, garantindo uma experiência de usuário contínua, permitindo uma troca eficiente de dados e informações entre o

SONDA Hybrid e outras plataformas empresariais, incluindo ferramentas de gerenciamento de ciclo de vida, ferramentas de monitoramento e ITSM (Projeto Especial). Além disso, possui APIs abertas e extensíveis que permitem aos desenvolvedores estender e personalizar as capacidades do **SONDA** Hybrid de acordo com as necessidades específica do **CLIENTE**.

Nossa plataforma é composta por três módulos que se complementam, proporcionando uma visão abrangente e integrada da infraestrutura de TI. Com essa abordagem, os **CLIENTES** terão acesso a insights valiosos e uma compreensão holística do seu ambiente tecnológico, permitindo uma gestão mais eficiente e estratégica.

5.1. Módulo de Orquestração

5.1.1. Provisionamento de Recursos

- Provisionamento fácil e rápido de máquinas virtuais, redes e armazenamento em uma variedade de ambientes de nuvem, incluindo AWS, Azure, Google Cloud Platform, e muito mais;
- Catálogo de serviços personalizável que permite aos usuários solicitar e provisionar recursos de acordo com suas necessidades específicas, com a capacidade de definir políticas de aprovação e limites de uso;
- Seleção de instâncias de máquinas virtuais com base nos requisitos de computação, memória, armazenamento e rede;
- Ajuste do tamanho das instâncias de máquinas virtuais e recursos de acordo com os requisitos de carga de trabalho, evitando recursos excessivamente dimensionados. Além da possibilidade de implementação de políticas de dimensionamento automático para escalar verticalmente conforme necessário;
- Todas os serviços de IaaS em um único ambiente com interface fácil e intuitiva para auxiliar o **CLIENTE** em todo o ciclo: desde a contratação do serviço (Experiência de carrinho de compras), gerenciamento e controle de faturamento.
- Permite o uso de modelos de provisionamento, incluindo modelos nativos da plataforma multicloud, automação simultânea de provisionamento, adoção de políticas relacionadas aos modelos de provisionamento, agendar tarefas, implementar fluxos de trabalho de orquestração baseada em eventos;

Gerenciamento de Instâncias

- Exibir o custo estimado da instância com base na configuração selecionada durante o pedido;
- Criar ou reiniciar instâncias;
- Iniciar, parar ou encerrar instâncias;
- Log de auditoria de instância;
- SSH nas instâncias;
- Redimensionar a configuração da instância (como CPU, RAM, DISCO) de acordo com o requisito;
- Visualizar dados de utilização históricos e atuais;
- Configurar tags;
- Visualizar uso para todas as instâncias;
- Informes de consumo online;

- Disponibilizar o download de todos os informes de consumo em .csv e Excel.

Gerenciamento de Armazenamento em Bloco

- Criar e anexar um novo volume de bloco a partir do catálogo de serviços;
- Excluir um volume de bloco a partir do catálogo de serviços.

Gerenciamento de Endereço IP Estático

- Configurar o endereço IP público estático para uma interface de rede;

Gerenciamento de Banco de Dados

- Configurar e criar VMs para Banco de Dados;

Gerenciamento de Scripts

- Entrega a possibilidade de gerenciamento de scripts;
- Visualizar logs de script,

Gerenciamento de Rede Virtual

- Configurar e criar uma Rede Virtual;
- Pesquisar e excluir a Rede Virtual,

5.1.2. Automação de Tarefas através do Catálogo de Serviços

- Criação e execução de fluxos de trabalhos automatizados para simplificar processos operacionais e reduzir a dependência de intervenção manual;
- É possível automatizar tarefas operacionais rotineiras, com biblioteca de fluxos de trabalho pré-construídos para tarefas comuns, permitindo aos usuários iniciar rapidamente a automação de processos.

5.1.3. Gerenciamento de Assinaturas

- Essa funcionalidade permite que o **CLIENTE** visualize e administre todas as suas assinaturas de forma centralizada.
- Aumentar ou reduzir a quantidade de uma assinatura;
- Ativar, suspender, reativar ou cancelar qualquer atribuição de serviço ao(s) usuário(s);
- Atribuir um único serviço a vários usuários;
- Atribuir vários serviços a um único usuário ao mesmo tempo;
- Os serviços podem ser atribuídos a uma organização ou a um usuário final, dependendo da natureza do serviço;
- Aumentar ou reduzir assinaturas;
- Cancelar assinaturas;

5.1.4. Gerenciamento de Configuração

- O **SONDA** Hybrid oferece gerenciamento centralizado de configurações de infraestrutura, permitindo a padronização e consistência em toda a infraestrutura de TI;

- Integra com as ferramentas de orquestração de container e infraestrutura (OpenShift, Terraform e Ansible e etc.).

5.1.5. Segurança

- Implementação de políticas de segurança granulares (controle de acesso) para proteger recursos e dados sensíveis em toda a infraestrutura de nuvem;
- Auditoria e rastreamento de atividades para garantir conformidade com regulamentos e padrões de segurança;
- Possibilita a adoção de boas práticas de segurança, como criptografia de dados, gerenciamento de chaves, controle de acesso e monitoramento de atividades;

5.1.6. Gestão de usuários e perfis de Acessos

- Permite a criação e gestão de usuários para compartilhamento de ambiente e personalização de perfis e departamentos com diferentes níveis de acesso de acordo com a necessidades das áreas de negócio e cotas de gastos;
- Permite adicionar, modificar, suspender e excluir usuários;

5.1.7. Chargeback

O consumo dos recursos de nuvem estará disponível para o **CLIENTE** no portal, através de relatórios, onde é possível realizar a visualização por custo, localidade ou cloud contratada pelo **CLIENTE**. Os relatórios facilitam e ajudam na gestão de seus serviços para ter sempre o controle e tomar as melhores decisões baseado em dados.

O Chargeback permite:

- Visualizar a lista com todos os recursos que estão em uso pelo **CLIENTE**;
- Centraliza todas as informações de custos: por recursos, histórico de consumo e armazenamento. Permitindo que os usuários tenham visibilidade dos custos de nuvem mais detalhados com base em parâmetros como: tipo, recursos por região, tipo de uso, etc.;
- Apresenta também informações de custos dos recursos que o usuário realizou a marcação da funcionalidade de Tag no **SONDA** Hybrid. A alocação de custos baseada em tags envolve a análise e a associação dos custos com categorias específicas (por exemplo, departamento, projeto, centro de custo) para fornecer a visibilidade detalhada dos custos e garantir a governança.

5.1.8. Relatórios

O **SONDA** Hybrid fornece para os usuários várias opções de relatórios padrão pré-definidos em HTML e .csv e Excel;

5.2. Módulo de FinOps

Gerenciar os custos em um ambiente multicloud é um dos maiores desafios para as empresas. Nesse contexto, o FinOps — prática de gestão financeira aplicada às operações de TI — torna-se essencial. O **SONDA** Hybrid integra um ecossistema de FinOps que oferece visibilidade dos gastos com TI, permitindo que as empresas monitorem seus custos de forma proativa e tomem decisões financeiras mais assertivas. Essa governança financeira alinhada às metas do negócio permite que as organizações otimizem o uso de

recursos em diferentes ambientes de TI sem comprometer a inovação e a agilidade necessárias para manter a competitividade no mercado.

O módulo de FinOps contempla:

- Centralização do billing multicloud em uma única plataforma;
- Consolidação de faturas de diferentes provedores em um formato unificado;
- Acompanhamento da evolução mensal dos custos por provedor;
- Detalhamento de consumo por provedor, serviço, recurso ou tags;
- Rateio e alocação de custos por tags, permitindo a alocação por categorias (departamento, projeto, centro de custo), garantindo visibilidade e governança;
- Recursos de visualizações para acompanhar tendências de gastos e gerar projeções baseadas no uso histórico.
- Recomendações de otimização, savings plans ou desligamento de recursos ociosos;
- Identificação de recursos subutilizados para redução de desperdícios;
- Comparação entre gastos realizados e orçados, com relatórios de variação;
- Dashboard com interface simples, com gráficos claros e métricas estratégicas, para apoiar decisões rápidas e inteligentes.
- Relatórios automatizados para áreas financeira, técnica e executiva;

5.3. Módulo de Conformidade e Auditoria

O aumento da utilização de infraestrutura multicloud intensifica a complexidade na gestão dos ambientes.

Com o **SONDA** Hybrid, é possível criar uma visualização automatizada da sua arquitetura de nuvem atual, economizando tempo e energia, além de reduzir o risco de erros. Por meio de diagramas e relatórios, você pode acessar todos os detalhes relevantes dos seus componentes e aplicativos em nuvem, incluindo configurações, interfaces de rede, grupos de segurança, tags, configurações de inicialização, avisos e muito mais. Além disso, a ferramenta permite identificar rapidamente configurações incorretas ou potenciais problemas de segurança, e inclui os resultados da avaliação de regras de conformidade definidas conforme a necessidade dos **CLIENTES**.

O módulo contempla:

- Inventário e Recomendações
  - Levantamento detalhado de todo o inventário do ambiente do cliente;
  - Recomendações e análise de vulnerabilidade;
  - Revisão das práticas de governança e Compliance, como HIPAA e PCI;
- Geração automática de diagramas de arquitetura e relatórios de auditoria, conformidade e segurança;
- Geração automática de documentos com exportação completa dos ativos de nuvem para ambientes Azure, AWS e GCP, otimizando tempo e reduzindo esforço manual.
- Possibilita a implementação de políticas de conformidade e auditoria, assegurando que **o** ambiente de cloud esteja alinhado a regulamentos e padrões de segurança

6. Ofertas

O **SONDA** Hybrid é composto por três módulos integrados: Orquestração, FinOps e Auditoria e Conformidade. Juntos, eles proporcionam uma visão completa e estratégica para os clientes.

Os módulos são: Orquestração, FinOps e Auditoria e Conformidade.

7. Segurança - Serviços de Segurança Gerenciados

A segurança da Plataforma **SONDA** Hybrid engloba os itens de Segurança listados abaixo:

- **Conformidade**

A Plataforma **SONDA** Hybrid é auditada e certificada com base nos padrões de segurança da informação relacionado as normas ISO 27001, 27017 e 27018.

- **Certificado Digital**

O **SONDA** Hybrid possui um certificado SSL válido, no qual todas as requisições HTTP são redirecionadas para HTTPS, incluindo todos os subdomínios e hostnames.

O HTTPS ajuda a evitar que dados sejam alterados durante a comunicações entre os websites e os navegadores dos usuários, garantindo:

  - Integridade: garante que as mensagens não foram alteradas durante comunicação;
  - Confidencialidade: a mensagem será lida apenas pelo destinatário real;
  - Autenticação: comprovação de que o servidor é realmente o servidor esperado.

- **Criptografia**

A criptografia no HTTPS funciona com um par de chaves, sendo uma chave pública e outra privada. Cada vez que um usuário solicita uma conexão ao site, o servidor envia a chave pública para este usuário. Com esta chave, o usuário tem a garantia de que toda a comunicação chegará apenas para o servidor, já que a chave privada se encontra no servidor.

- **Identidades gerenciadas**

Gerenciamos das credenciais de acesso dos profissionais **SONDA** é realizado através de uma solução de cofre de senha que fornece uma maneira de armazenar com segurança as credenciais.

Nossos analistas e especialista não conhecem e não tem posse da senha para autenticar nas instâncias virtuais. A senha é alterada após cada solicitação de uso.

Nota: Para os acessos do **CLIENTE** no portal **SONDA** Hybrid é realizado o levantamento e criação em fase de projeto. Para resolução de problemas, criação, alteração ou exclusão de usuário deve ser aberto um chamado por profissionais autorizados do **CLIENTE**.

- **Política de senha do usuário**

A construção de qualquer senha deve considerar o uso e a composição entre caracteres alfabéticos, maiúscu-los, minúsculos, números e alfanuméricos. Toda senha deve ter no mínimo 14 (quatorze) caracteres, por exemplo: Abcd$125de3647.

A senha não poderá repetir nenhuma das últimas 13 (treze) senhas já previamente utilizadas.

- **Controle de acesso baseado em função**

Podemos segmentar as tarefas dentro da equipe e permitir apenas as ações necessárias baseada na função.

- **Anti-DDoS**

A **SONDA** atua com uma solução de Anti-DDoS on-premise para mitigação de ataques de aplicação tais como: TCP Syn Flood, TCP RST Flood, TCP FIN Flood, TCP ACK Flood, ICMP Flood, UDP Flood, UDP Amplify.

Além disso, quando um ataque volumétrico de grande escala é iniciado, o "Scrubing Center" da **SONDA** é acionado – um centro de mitigação de ataques localizado fora do Data Center - que desvia todo o tráfego para este centro. A partir disso, o que é considerado ataque será descartado e o tráfego válido será devolvido para a rede e encaminhado normalmente para o destino.

- **Firewall e IPS**

Utilizamos um firewall "next generation", que contribui para a capacidade do serviço de prevenir, detectar e responder a incidentes de segurança. Além de ser responsável pela configuração e segurança da rede.

A proteção aplicada permite filtrar as comunicações por aplicação, atuando diretamente na Camada 7. Desta forma, o firewall consegue identificar os tipos de aplicação e conexão que trafegam no ambiente e inferir se esses casos tratam de acessos legítimos ou não.

Como forma de complementar à análise, são aplicados o IDS (Sistema de Detecção de Intrusão) e o IPS (Sistema de Prevenção de Intrusão) no ambiente, a fim de avaliar as assinaturas de todas as conexões e identificar possíveis acessos indevidos.

- **Segurança Física**

O Data Center **SONDA** possui equipe de segurança física em Regime 24x7, Portaria Blindada, Controle de Acesso em todas as portas, sendo a entrada no Data Center controlada com dupla autenticação (Cartão + Biometria), Mais de 100 Câmeras de alta resolução em todo a edificação além de sistema de Monitoramento e Gravação de Imagens.

- **Segurança de Rede Interna – SONDA**

A infraestrutura de rede interna da **SONDA** conta com vários recursos para garantir a segregação de seus **CLIENTES** e dados, com uma arquitetura preparada para um ambiente multi-locatário.

7.1. Notificação de Incidente de Segurança

Incidente de segurança é qualquer ocorrência que possa comprometer o bom andamento dos sistemas da **SONDA** e dos seus **CLIENTES.** Exemplos incluem o uso não autorizado de senhas, a adulteração de informações em um banco de dados, o envio ou recepção de mensagens ameaçadoras, roubo de informação, ocorrência de vírus, ou qualquer outro fato que contrarie as disposições dessa política.

Qualquer incidente de segurança deve ser reportado à Equipe de Segurança de informação através do e-mail segurancainfo.qualidade@sonda.com.

Os incidentes recebidos por este canal serão analisados pela equipe de Segurança da Informação da **SONDA**, de acordo com as diretrizes organizacionais e melhores práticas internacionais.

8. Premissas e Restrições

8.1. Premissas

As premissas do produto em relação ao **CLIENTE** são:

- Fornecer as credenciais de acesso às diferentes plataformas a serem integradas na solução;
- Entregar toda a informação necessária para a análise de requerimentos com o objetivo de entregar a melhor solução;
- Implantar, gerenciar, manter, corrigir e/ou atualizar os aplicativos implantados.
- As licenças incluídas no produto estão ligadas somente a plataforma (Plataforma **SONDA** Hybrid – Módulo de Orquestração, Finops e Conformidade e Auditoria), nelas não estão incluídas qualquer licença além do **SONDA** Hybrid;
- O **SONDA** Hybrid possui integração com os principais provedores de nuvem (AWS, Azure, GCP, IBM Cloud e Huawei);
- Caso o **CLIENTE** queira incluir máquinas utilizadas pelo Host Virtual Compartilhado da **SONDA**, o uso deve ser avaliado pela **SONDA**.

Restrições

- Todos os serviços de segurança citados se referem somente ao acesso ao portal **SONDA** Hybrid;
- O acesso e segurança do **CLIENTE** ao seu ambiente de cloud pública contratado não é contemplado neste produto;
- As máquinas criadas de maneira externas ao portal **SONDA** Hybrid serão inventariadas e bilhetadas pela ferramenta, assim como as criadas pelo portal.

8.2. Pré Requisitos para integração das subscrições do CLIENTE ao SONDA Hybrid:

- **Azure**

A integração do **SONDA** Hybrid requer acesso de Owner (Proprietário) ou Contributor (Colaborador) à assinatura, por meio de um App Registration. Ao adicionar uma ou mais nuvens Azure ao **SONDA** Hybrid, serão necessárias as seguintes informações:

- Azure Subscription ID
- Directory (tenant) ID
- Application (client) ID
- Application (client) Secret
- A aplicação (client) deve ter função de Owner ou Contributor na assinatura

Para contas CSP, são necessárias informações adicionais:

- CSP Directory (tenant) ID
- CSP Application (client) ID

- CSP Application (client) Secret (Web App Key)

O appliance do **SONDA** Hybrid precisa de acesso HTTPS (porta 443) de saída para os endpoints do Azure. Dependendo do tipo de nuvem Azure escolhida, é necessário garantir que os endpoints corretos estejam liberados.

Credenciais e Permissões

O **SONDA** Hybrid realiza a autenticação com o Azure por meio de um App Registration, que deve possuir função de Owner ou Contributor na assinatura.

Atenção: O uso de um App Registration (service principal) com permissões seletivas em recursos específicos, que não seja Owner ou Contributor da assinatura, não é suportado e causará falhas ou problemas na integração.

- **AWS**

  - Credenciais de Segurança IAM da AWS
    - Access Key e Secret Key com privilégios de usuário suficientes;
  - AWS IAM Permissions: Abaixo estão as permissões do AWS IAM necessárias para os serviços SONDA Hybrid.
    - autoscaling
      - "autoscaling:AttachInstances",
      - "autoscaling:AttachLoadBalancerTargetGroups",
      - "autoscaling:CreateAutoScalingGroup",
      - "autoscaling:DeleteAutoScalingGroup",
      - "autoscaling:DeleteLaunchConfiguration",
      - "autoscaling:DeletePolicy",
      - "autoscaling:DescribeAutoScalingGroups",
      - "autoscaling:DescribeLaunchConfigurations",
      - "autoscaling:DescribeLoadBalancers",
      - "autoscaling:DescribePolicies",
      - "autoscaling:DetachInstances",
      - "autoscaling:PutScalingPolicy",
      - "autoscaling:UpdateAutoScalingGroup",
    - **cloudformation**
      - "cloudformation:CreateStack",
      - "cloudformation:DeleteStack",
      - "cloudformation:DescribeStackEvents",
      - "cloudformation:DescribeStackResources",
      - "cloudformation:DescribeStacks",
      - "cloudformation:GetTemplate",
      - "cloudformation:UpdateStack",
      - "cloudformation:ValidateTemplate",
    - **cloudwatch**
      - "cloudwatch:DeleteAlarms",
      - "cloudwatch:DescribeAlarms",

        - "cloudwatch:GetMetricStatistics",
        - "cloudwatch:PutMetricAlarm",
    - **costexplorer**
        - "ce:*",
    - **Cost and Usage Reports**
        - "cur:DescribeReportDefinitions",
        - "cur:PutReportDefinition",
    - **ec2**
        - "ec2:AllocateAddress",
        - "ec2:AssignPrivateIpAddresses",
        - "ec2:AssociateAddress",
        - "ec2:AttachInternetGateway",
        - "ec2:AttachNetworkInterface",
        - "ec2:AttachVolume",
        - "ec2:AuthorizeSecurityGroupEgress",
        - "ec2:AuthorizeSecurityGroupIngress",
        - "ec2:CancelExportTask",
        - "ec2:CancelImportTask",
        - "ec2:CopyImage",
        - "ec2:CopySnapshot",
        - "ec2:CreateEgressOnlyInternetGateway",
        - "ec2:CreateImage",
        - "ec2:CreateInstanceExportTask",
        - "ec2:CreateInternetGateway",
        - "ec2:CreateKeyPair",
        - "ec2:CreateNatGateway",
        - "ec2:CreateNetworkAcl",
        - "ec2:CreateNetworkAclEntry",
        - "ec2:CreateNetworkInterface",
        - "ec2:CreateRoute",
        - "ec2:CreateSecurityGroup",
        - "ec2:CreateSnapshot",
        - "ec2:CreateSubnet",
        - "ec2:CreateTags",
        - "ec2:CreateVolume",
        - "ec2:CreateVpc",
        - "ec2:DeleteEgressOnlyInternetGateway",
        - "ec2:DeleteInternetGateway",
        - "ec2:DeleteKeyPair",
        - "ec2:DeleteNatGateway",
        - "ec2:DeleteNetworkAcl",
        - "ec2:DeleteNetworkAclEntry",
        - "ec2:DeleteNetworkInterface",
        - "ec2:DeleteRoute",
        - "ec2:DeleteSecurityGroup",

- "ec2:DeleteSnapshot",
- "ec2:DeleteSubnet",
- "ec2:DeleteTags",
- "ec2:DeleteVolume",
- "ec2:DeleteVpc",
- "ec2:DeregisterImage",
- "ec2:DescribeAccountAttributes",
- "ec2:DescribeAddresses",
- "ec2:DescribeAvailabilityZones",
- "ec2:DescribeClassicLinkInstances",
- "ec2:DescribeClientVpnConnections",
- "ec2:DescribeClientVpnEndpoints",
- "ec2:DescribeConversionTasks",
- "ec2:DescribeEgressOnlyInternetGateways",
- "ec2:DescribeExportTasks",
- "ec2:DescribeImageAttribute",
- "ec2:DescribeImages",
- "ec2:DescribeImportImageTasks",
- "ec2:DescribeImportSnapshotTasks",
- "ec2:DescribeInstances",
- "ec2:DescribeInstanceStatus",
- "ec2:DescribeInstanceTypes",
- "ec2:DescribeInternetGateways",
- "ec2:DescribeKeyPairs",
- "ec2:DescribeNatGateways",
- "ec2:DescribeNetworkAcls",
- "ec2:DescribeNetworkInterfaceAttribute",
- "ec2:DescribeNetworkInterfaces",
- "ec2:DescribeRegions",
- "ec2:DescribeRouteTables",
- "ec2:DescribeSecurityGroupReferences",
- "ec2:DescribeSecurityGroups",
- "ec2:DescribeSnapshotAttribute",
- "ec2:DescribeSnapshots",
- "ec2:DescribeStaleSecurityGroups",
- "ec2:DescribeSubnets",
- "ec2:DescribeTags",
- "ec2:DescribeTransitGateways",
- "ec2:DescribeTransitGatewayVpcAttachments",
- "ec2:DescribeVolumeAttribute",
- "ec2:DescribeVolumes",
- "ec2:DescribeVolumeStatus",
- "ec2:DescribeVpcAttribute",
- "ec2:DescribeVpcClassicLink",
- "ec2:DescribeVpcClassicLinkDnsSupport",

        - "ec2:DescribeVpcEndpoints",
        - "ec2:DescribeVpcEndpointServices",
        - "ec2:DescribeVpcPeeringConnections",
        - "ec2:DescribeVpcs",
        - "ec2:DescribeVpnGateways",
        - "ec2:DetachInternetGateway",
        - "ec2:DetachNetworkInterface",
        - "ec2:DetachVolume",
        - "ec2:DisassociateAddress",
        - "ec2:GetPasswordData",
        - "ec2:ImportImage",
        - "ec2:ImportInstance",
        - "ec2:ImportKeyPair",
        - "ec2:ImportSnapshot",
        - "ec2:ImportVolume",
        - "ec2:ModifyImageAttribute",
        - "ec2:ModifyInstanceAttribute",
        - "ec2:ModifyNetworkInterfaceAttribute",
        - "ec2:ModifySnapshotAttribute",
        - "ec2:ModifySubnetAttribute",
        - "ec2:ModifyVolumeAttribute",
        - "ec2:RebootInstances",
        - "ec2:RegisterImage",
        - "ec2:ReleaseAddress",
        - "ec2:ReplaceNetworkAclAssociation",
        - "ec2:ReplaceNetworkAclEntry",
        - "ec2:ResetImageAttribute",
        - "ec2:ResetInstanceAttribute",
        - "ec2:ResetNetworkInterfaceAttribute",
        - "ec2:ResetSnapshotAttribute",
        - "ec2:RevokeSecurityGroupEgress",
        - "ec2:RevokeSecurityGroupIngress",
        - "ec2:RunInstances",
        - "ec2:StartInstances",
        - "ec2:StopInstances",
        - "ec2:TerminateInstances",
        - "ec2:UnassignPrivateIpAddresses",
        - "ec2:UpdateSecurityGroupRuleDescriptionsEgress",
    - **eks**
        - "eks:*",
    - **elasticloadbalancing**
        - "elasticloadbalancing:AddTags",
        - "elasticloadbalancing:ApplySecurityGroupsToLoadBalancer",
        - "elasticloadbalancing:AttachLoadBalancerToSubnets",
        - "elasticloadbalancing:CreateListener",

        - "elasticloadbalancing:CreateLoadBalancer",
        - "elasticloadbalancing:CreateRule",
        - "elasticloadbalancing:CreateTargetGroup",
        - "elasticloadbalancing:DeleteListener",
        - "elasticloadbalancing:DeleteLoadBalancer",
        - "elasticloadbalancing:DeleteRule",
        - "elasticloadbalancing:DeleteTargetGroup",
        - "elasticloadbalancing:DescribeLoadBalancers",
        - "elasticloadbalancing:DescribeRules",
        - "elasticloadbalancing:DescribeTargetGroups",
        - "elasticloadbalancing:ModifyListener",
        - "elasticloadbalancing:ModifyTargetGroupAttributes",
        - "elasticloadbalancing:RegisterTargets",
        - "elasticloadbalancing:SetSecurityGroups",
        - "elasticloadbalancing:SetSubnets",
    - **elasticsearch**
        - "es:DescribeElasticsearchDomains",
        - "es:ListDomainNames",
    - **iam**
        -
        - "iam:ListGroups",
        - "iam:ListInstanceProfiles",
        - "iam:ListRoles",
    - **kms**
        - "kms:Decrypt",
        - "kms:GenerateDataKey",
    - **rds**
        - "rds:AddRoleToDBCluster",
        - "rds:AddTagsToResource",
        - "rds:ApplyPendingMaintenanceAction",
        - "rds:AuthorizeDBSecurityGroupIngress",
        - "rds:CopyDBClusterSnapshot",
        - "rds:CopyDBParameterGroup",
        - "rds:CopyDBSnapshot",
        - "rds:CreateDBCluster",
        - "rds:CreateDBClusterSnapshot",
        - "rds:CreateDBInstance",
        - "rds:CreateDBInstanceReadReplica",
        - "rds:CreateDBSecurityGroup",
        - "rds:CreateDBSnapshot",
        - "rds:DeleteDBCluster",
        - "rds:DeleteDBInstance",
        - "rds:DeleteDBSecurityGroup",
        - "rds:DeleteDBSnapshot",
        - "rds:DescribeAccountAttributes",

- "rds:DescribeCertificates",
- "rds:DescribeDBClusterParameterGroups",
- "rds:DescribeDBClusterParameters",
- "rds:DescribeDBClusters",
- "rds:DescribeDBClusterSnapshotAttributes",
- "rds:DescribeDBClusterSnapshots",
- "rds:DescribeDBEngineVersions",
- "rds:DescribeDBInstances",
- "rds:DescribeDBLogFiles",
- "rds:DescribeDBParameterGroups",
- "rds:DescribeDBParameters",
- "rds:DescribeDBSecurityGroups",
- "rds:DescribeDBSnapshotAttributes",
- "rds:DescribeDBSnapshots",
- "rds:DescribeDBSubnetGroups",
- "rds:DescribeEngineDefaultClusterParameters",
- "rds:DescribeEngineDefaultParameters",
- "rds:DescribeEventCategories",
- "rds:DescribeEvents",
- "rds:DescribeOptionGroupOptions",
- "rds:DescribeOptionGroups",
- "rds:DescribeOrderableDBInstanceOptions",
- "rds:ListTagsForResource",
- "rds:ModifyDBCluster",
- "rds:ModifyDBClusterParameterGroup",
- "rds:ModifyDBClusterSnapshotAttribute",
- "rds:ModifyDBInstance",
- "rds:ModifyDBParameterGroup",
- "rds:ModifyDBSnapshotAttribute",
- "rds:PromoteReadReplica",
- "rds:RebootDBInstance",
- "rds:RemoveTagsFromResource",
- "rds:RestoreDBClusterFromSnapshot",
- "rds:RestoreDBClusterToPointInTime",
- "rds:RestoreDBInstanceFromDBSnapshot",
- "rds:RestoreDBInstanceToPointInTime",
- "rds:RevokeDBSecurityGroupIngress",
- "rds:StartDBInstance",
- "rds:StopDBInstance",

- **route53**
  - "route53:ChangeResourceRecordSets",
  - "route53:GetHostedZone",
  - "route53:ListHostedZones",
  - "route53:ListResourceRecordSets",
- **s3**

        - "s3:AbortMultipartUpload",
        - "s3:CreateBucket",
        - "s3:DeleteBucket",
        - "s3:DeleteObject",
        - "s3:DeleteObjectVersion",
        - "s3:GetBucketLocation",
        - "s3:GetBucketPolicy",
        - "s3:GetObject",
        - "s3:GetObjectVersion",
        - "s3:ListAllMyBuckets",
        - "s3:ListBucket",
        - "s3:ListBucketMultipartUploads",
        - "s3:ListBucketVersions",
        - "s3:ListMultipartUploadParts",
        - "s3:PutBucketPolicy",
        - "s3:PutObject",
    - **Systems Manager**
        - "ssm:GetParameters",

- **Google**

Para integrar o **SONDA** Hybrid com o Google Cloud Platform (GCP), são necessários os seguintes pré-requisitos:

- Credenciais de uma conta de serviço IAM com permissões de Owner ou Compute Admin
- Chave privada e e-mail do cliente da conta de serviço
- As APIs devem estar ativadas em “APIs & Services” e precisam estar habilitadas para todos os projetos ou para o projeto selecionado, dependendo das configurações da sua integração com o GCP Cloud.
- A próxima seção contém instruções detalhadas sobre como ativar as APIs no console web do GCP.
- As seguintes APIs devem estar ativadas:
- Compute Engine API
- Cloud Resource Manager API
- Cloud Billing API
- Identity and Access Management (IAM) API
- BigQuery API
- BigQuery Data Transfer API

- **OCI**

Integrar a Oracle Public Cloud ao **SONDA** Hybrid requer acesso a uma conta de serviço com, no mínimo, o conjunto de permissões listado abaixo. Requisitos de Políticas da Oracle Cloud

- Permitir que o grupo <GRUPO QUE CONTÉM O USUÁRIO DE SERVIÇO> gerencie cluster-family no compartimento <COMPARTIMENTO ESCOLHIDO OU COMPARTIMENTO RAIZ>

- Permitir que o grupo <GRUPO QUE CONTÉM O USUÁRIO DE SERVIÇO> gerencie compute-management-family no compartimento <COMPARTIMENTO ESCOLHIDO OU COMPARTIMENTO RAIZ>
- Permitir que o grupo <GRUPO QUE CONTÉM O USUÁRIO DE SERVIÇO> gerencie data-catalog-family no compartimento <COMPARTIMENTO ESCOLHIDO OU COMPARTIMENTO RAIZ>
- Permitir que o grupo <GRUPO QUE CONTÉM O USUÁRIO DE SERVIÇO> gerencie dns no compartimento <COMPARTIMENTO ESCOLHIDO OU COMPARTIMENTO RAIZ>
- Permitir que o grupo <GRUPO QUE CONTÉM O USUÁRIO DE SERVIÇO> gerencie file-family no compartimento <COMPARTIMENTO ESCOLHIDO OU COMPARTIMENTO RAIZ>
- Permitir que o grupo <GRUPO QUE CONTÉM O USUÁRIO DE SERVIÇO> gerencie instance-family no compartimento <COMPARTIMENTO ESCOLHIDO OU COMPARTIMENTO RAIZ>
- Permitir que o grupo <GRUPO QUE CONTÉM O USUÁRIO DE SERVIÇO> gerencie object-family no compartimento <COMPARTIMENTO ESCOLHIDO OU COMPARTIMENTO RAIZ>
- Permitir que o grupo <GRUPO QUE CONTÉM O USUÁRIO DE SERVIÇO> gerencie virtual-network-family no compartimento <COMPARTIMENTO ESCOLHIDO OU COMPARTIMENTO RAIZ>
- Permitir que o grupo <GRUPO QUE CONTÉM O USUÁRIO DE SERVIÇO> gerencie volume-family no compartimento <COMPARTIMENTO ESCOLHIDO OU COMPARTIMENTO RAIZ>

IMPORTANTE: Um par de chaves (tanto a chave pública quanto a privada) deve ser adicionado ao HPE Morpheus Enterprise com a chave pública no formato ssh-rsa. A chave pública no formato PEM precisa ser adicionada às chaves dos usuários no console da Oracle Cloud para autenticação.

OBSERVAÇÃO: Informações sobre como fazer o upload da chave pública e gerar o OCID do Tenancy e o OCID do Usuário podem ser encontradas em:
https://docs.cloud.oracle.com/iaas/Content/API/Concepts/apisigningkey.htm

Os pré-requisitos para integração das subscrições do **CLIENTE** ao **SONDA** Hybrid estão sujeitas a atualizações frequentes, refletindo eventuais mudanças ou aprimoramentos nos processos descritos. Para acessar a versão mais completa e atualizada, recomenda-se consultar o conteúdo integral disponível no seguinte link: Clouds | HPE Morpheus Enterprise Software Documentation v8.0.7

8.1. Pré Requisitos para integração do SONDA Hybrid ao ambiente on premisse:

Para que o **SONDA** Hybrid seja integrado ao ambiente on-premise do **CLIENTE,** os requisitos principais envolvem rede, credenciais, permissões e conectores.

- **Requisitos de Conectividade de Rede**

Para que o SONDA Hybrid consiga inventariar, provisionar, monitorar e automatizar recursos do ambiente on-premise, é necessário:

  - Conectividade IP bidirecional: entre o SONDA Hybrid e o ambiente do **CLIENTE** — seja via:
    - VPN site-to-site;
    - MPLS / SD-WAN;
    - Link dedicado;

        - IPs públicos com regras de firewall bem definidas.
    - Portas abertas, principalmente:
        - 443/TCP: comunicação HTTPS entre appliance e endpoints (hipervisores, agentes, APIs etc.)
        - 22/TCP: SSH para instalação de agentes em hosts Linux (quando aplicável)
        - 5985/5986: WinRM HTTP/HTTPS para hosts Windows (quando aplicável)
        - Portas específicas dos hipervisores / storage / ferramentas: (ex: vCenter, Nutanix Prism, API do OpenStack, etc.)

Importante: o **SONDA** Hybrid sempre atua como "controlador central", então ele precisa alcançar os endpoints do **CLIENTE** — seja via IP interno (via VPN/MPLS) ou IP público com segurança controlada.

- **Requisitos de Integração com Virtualizadores ou Plataformas**

Dependendo do que o **CLIENTE** tem on-premise, será necessário configurar as Clouds no SONDA Hybrid:

Ambiente on-premise	Requisitos para integração com SONDA Hybrid
VMware vCenter	URL ou IP acessível do vCenter + usuário com permissões de administrador (ou service account com RBAC adequado) + porta 443 liberada
Nutanix AHV	IP do Prism Central/Element + credenciais admin + porta 9440 (HTTPS) liberada
OpenStack	Endpoint da API Keystone + credenciais + portas HTTPS abertas
Hyper-V	IP ou hostname do host Hyper-V ou do System Center Virtual Machine Manager (SCVMM) + credenciais administrativas (domínio ou local) + portas WinRM (5985/5986) e 443 liberadas
OpenShift	Endpoint da API do cluster OpenShift (URL do API Server) + token de acesso ou credenciais com permissões adequadas + portas HTTPS abertas + certificado válido ou CA confiável configurada

- **Requisitos de Credenciais e Permissões**
    - Conta de serviço dedicada para integração com hypervisors (ex: `sondahybrid-admin@cliente.local`).
    - Permissões de leitura e escrita (inventário + provisionamento).
    - Para VMware, recomenda-se perfil de acesso com:
        - Inventário completo (vCenter, datastores, networks);
        - Provisionamento de VMs;
        - Criação/remoção de snapshots;
        - Gestão de templates.
- **Agentes SONDA Hybrid (opcional, mas recomendado)**
    - O **SONDA** Hybrid pode funcionar agentless (via API/SSH/WinRM), mas para gestão avançada (scripts, monitoramento, backups etc.) é recomendado instalar o agente em cada host/VM.
    - Esses agentes se comunicam de dentro do **CLIENTE** para o appliance, usando HTTPS (porta 443).

  - Portanto, o firewall do **CLIENTE** deve permitir saída HTTPS para o FQDN/IP do **SONDA** Hybrid.
- **DNS, Certificados e Segurança**
  - DNS interno do **CLIENTE** deve resolver corretamente os nomes dos hypervisores, vCenter, etc., para que o **SONDA** Hybrid consiga se conectar.
  - O **SONDA** Hybrid deve ser acessível por um FQDN confiável (por exemplo `sondahybrid.empresa.com.br`) — de preferência com certificado SSL/TLS válido.
  - Caso use VPN, garanta que as rotas internas estejam bem configuradas e que não haja NAT que quebre a comunicação dos agentes.
- **Checklist resumido para integração com ambiente do CLIENTE**
  - [ ] Conectividade VPN/MPLS ou portas públicas abertas com firewall controlado
  - [ ] Porta 443 do **SONDA** Hybrid acessível a partir do ambiente do **CLIENTE**
  - [ ] Acesso do **SONDA** Hybrid às APIs e hosts on-premise (vCenter, Nutanix, OpenStack, hosts, etc.)
  - [ ] Credenciais administrativas (service accounts) configuradas
  - [ ] DNS e SSL configurados corretamente
  - [ ] (Opcional) Permitir instalação dos agentes SONDA Hybrid em VMs/hosts para maior funcionalidade
  - [ ] Verificar permissões em firewalls internos e proxies corporativos
- **Monitoramento, Backup e ITSM**

O **SONDA** Hybrid conta com um conjunto de integrações padrão que garantem maior eficiência, visibilidade e governança das operações. Atualmente, as ferramentas homologadas são:

- Backup: Commvault e Veritas
- ITSM: Aranda e CA Service Desk
- Monitoramento: SolarWinds

Essas integrações asseguram a padronização dos processos, a centralização das informações e o alinhamento com as melhores práticas de gestão de ambientes híbridos.

A integração com ambientes on-premises requer uma análise prévia, uma vez que há pré-requisitos técnicos que devem ser verificados para garantir a viabilidade e a conformidade da solução.

Eventuais demandas fora do padrão estabelecido serão avaliadas individualmente e poderão exigir horas adicionais de consultoria e/ou desenvolvimento, conforme a complexidade identificada.

9. Matriz de Responsabilidades

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

Contratação Opcional?	Atividades	SONDA	CLIENTE
Não	Gestão do Portal	-	R
Não	Gestão de Subscrições	-	R
Não	Criar Tenant para o **CLIENTE**	R	I

Não	Gestão dos usuários do **CLIENTE** no portal	R	A

10.Requisição de Serviço

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
Suporte a dúvidas em relação a usabilidade do **SONDA** Hybrid	C	Conforme TS contratado


SONDA
make it easy