



MINISTÉRIO DAS CIDADES
Coordenação de Infraestrutura da Informação
ANEXO I - ESPECIFICAÇÕES TÉCNICAS

Item	Descrição	Métrica	Quantidade
1	Hardware otimizado para cloud privada	Unidade	8
2	Solução de cloud privada e software para gerenciamento de infraestrutura	Unidade de core	384

1. **Item 1 - Hardware otimizado para cloud privada**

1.1. Só serão aceitos hardwares certificados pelo fabricante da solução de cloud privada ofertada, de forma que seja garantida a compatibilidade com a ferramenta de gestão, atualização dos firmwares de maneira centralizada, automatizada e orquestrada.

1.2. Todos os componentes de hardware deverão ser totalmente compatíveis com os softwares especificados neste termo de referência.

1.3. Deverá ser um produto do segmento de servidores.

1.4. Deverá ser ofertado com o mínimo 2 processadores físicos.

1.5. Cada processador deverá conter no mínimo 24 núcleos.

1.6. Cada processador deverá ter frequência mínima de 2.6 GHz.

1.7. Cada processador deverá ter no mínimo 60 MB de cache.

1.8. Deverá ser da geração mais recente ofertada pelo fabricante do equipamento.

1.9. Deverá ser ofertado com o mínimo 1TB de memória RAM, sendo em pelo menos 16 (dezesseis) módulos de memória DDR4 com o mínimo 4800MHz de frequência.

1.10. Cada servidor deverá conter 2 placas dual-port 25Gbps SFP28 compatível com transceptores 25GB SFP28.

1.11. Cada servidor ou nó deverá prover no mínimo 60TB (sessenta) de capacidade de armazenamento bruta utilizando drives SSD ou NVMe.

2. **Item 2 - Solução de cloud privada e software para gerenciamento de infraestrutura**

2.1. Cada unidade deverá licenciar um núcleo de processamento para a solução de cloud e para o gerenciamento da infraestrutura.

2.2. A subscrição fornecida, deverá ser homologada e certificada pelo fabricante do hardware ofertado.

2.3. A solução de cloud privada deverá incluir virtualização de infraestrutura (computação, rede e armazenamento) e o respectivo gerenciamento configurado de maneira a garantir alta disponibilidade e sem ponto único de falha.

2.4. A solução deverá permitir a configuração de um cluster com todos os equipamentos deste termo de referência, mesmo com as diferentes especificações de seus componentes internos, sendo permitida também a adição de novos equipamentos futuramente com novas gerações de processadores, diferentes configurações de discos, memória RAM e a inclusão de novos equipamentos com GPU para atender demandas de inteligência artificial e aprendizado de máquina.

2.5. Permitir a realização de snapshots e clones através da solução de armazenamento de dados definida por software (SDS), independente do Hypervisor, utilizando algoritmo redirect-on-write para maior eficiência na utilização de storage bem como no tempo necessário para conclusão do snapshot ou clone.

- 2.6. Quando da inclusão online e não disruptiva de novos equipamentos com mais de uma camada de armazenamento (NVMe/SSD/HDD), o software deverá realizar a movimentação dos dados entre as camadas para favorecer o desempenho necessário aos dados mais acessados, garantindo a gestão do ciclo de vida dos dados (ILM) no nível do cluster.
- 2.7. A solução deverá permitir a definição do número de réplicas dos dados no mesmo cluster, sendo o dado original e uma réplica, em equipamentos distintos no mesmo cluster, para aplicações menos críticas e o dado original mais duas réplicas, em equipamentos distintos no mesmo cluster, para aplicações mais críticas.
- 2.8. A solução deverá permitir a configuração de domínios de disponibilidade de modo a tolerar a falha de equipamentos e racks. A falha de um disco não deve interromper ou impactar o funcionamento de outros discos na solução.
- 2.9. A subscrição de software deverá permitir a compressão de dados durante a sua ingestão e após o seu armazenamento na camada de capacidade.
- 2.10. O SDS deverá permitir a deduplicação global dos dados, tanto na camada de desempenho quanto na camada de capacidade, de modo que até a replicação dos dados para outro cluster seja otimizada para reduzir o uso de banda.
- 2.11. Deverá permitir a configuração de QoS de armazenamento para máquinas virtuais (VMs) a fim de limitar a utilização demasiada de recursos que pudesse interferir no funcionamento de outras VMs no mesmo cluster.
- 2.12. Permitir a priorização do uso da camada de maior desempenho do storage para determinadas VMs e seus respectivos discos virtuais através da interface gráfica de gestão.
- 2.13. Deverá permitir a configuração de armazenamento através de volumes iSCSI para VMs em execução no cluster e para aplicações externas ao cluster, inclusive bare-metal.
- 2.14. A subscrição deverá permitir a configuração de planos de proteção com retenção de snapshots locais e a replicação de dados otimizada para outro cluster com objetivo de ponto de recuperação (RPO) de pelo menos 1h (uma hora).
- 2.15. Deverá permitir a realização de snapshots através do SDS com consistência para os dados da aplicação (application-consistent), tanto para VMs com sistema operacional Windows como para VMs com sistema operacional Linux, através de tecnologia VSS e semelhantes.
- 2.16. Permitir que o próprio administrador da máquina virtual realize a recuperação granular de arquivos sem a necessidade de envolvimento da equipe responsável pela gestão das cópias de segurança (backup).
- 2.17. Deverá permitir a autenticação do cliente para que o cluster obtenha um certificado válido do usuário garantindo uma autenticação bidirecional em que o servidor também verifica a autenticidade do usuário através de um certificado válido fornecido por ele ao acessar a console de gestão.
- 2.18. Para aumento de segurança, a subscrição deverá permitir o bloqueio do cluster para restringir o acesso administrativo ao Hypervisor e SDS somente através do uso de chaves SSH, sem a utilização de senhas.
- 2.19. O software deverá permitir o uso da funcionalidade de segurança Windows Defender Credential Guard para isolamento das credenciais em máquinas virtuais com sistema operacional Windows, evitando ataques como Pass-the-Hash e Pass-The-Ticket.
- 2.20. O software deverá permitir o emprego de tecnologias como vGPU para compartilhamento de GPU entre desktops virtualizados e GPU passthrough para aplicações de inteligência artificial e aprendizagem de máquina virtualizadas e containerizadas.
- 2.21. O software deverá suportar o provisionamento automatizado, operações e a gestão do ciclo de vida de pelo menos três clusters Kubernetes prontos para ambiente de produção com alta disponibilidade utilizando mais de um master node, com ou sem um balanceador de carga externo. O cluster Kubernetes deve suportar o armazenamento persistente em modo de acesso Read-Write-Once para aplicativos em contêineres através de integração nativa com CSI driver para Volumes iSCSI e compartilhamento NFS, e Read-Write-Many para compartilhamento NFS. Também deverá ser possível a integração com o serviço de armazenamento de objetos através de protocolo S3. Deverá permitir operações de escalabilidade para aumento do número de worker nodes sem interrupção para os aplicativos e com a simplicidade de um clique através da interface gráfica. Suportar atualização de software dos nodes e do Kubernetes sem interrupção para os aplicativos de produção. Deverá suportar ferramentas para monitoramento, registro e alerta utilizando pilha EFK (Prometheus, Elasticsearch, Fluent Bit e Kibana) ou semelhantes.

- 2.22. A solução deverá permitir a configuração de redes Multi-tenant através do conceito de redes overlay (Virtual Private Cloud – VPC), garantindo isolamento de rede para segurança, sobreposição de endereços IP, auto-serviço para criação de redes virtuais, mobilidade de IP de máquinas virtuais e conectividade com nuvem híbrida.
- 2.23. A solução deverá permitir a gestão centralizada de múltiplos clusters no mesmo centro de dados e em centros distantes geograficamente para que seja possível gestão da infraestrutura, monitoramento de alertas e saúde destes clusters.
- 2.24. Deverá permitir a criação de projetos, estabelecendo quotas de recursos computacionais além do controle de acesso de usuários (Role Based Access Control - RBAC) de uma estrutura de diretório Active Directory ou LDAP com suas respectivas permissões.
- 2.25. Deverá permitir a autenticação em nível empresarial utilizando Role Based Access Control (RBAC), sendo possível atribuir diferentes níveis de permissão para usuários e grupos de usuários.
- 2.26. Deverá permitir a integração com outras tecnologias através de APIs do tipo REST.
- 2.27. A interface de gerenciamento web deverá possuir uma ferramenta de busca contextualizada para acelerar as pesquisas na interface gráfica.
- 2.28. O fabricante da solução deverá disponibilizar um portal de suporte para abertura de chamados, upload de logs e dados de diagnóstico relevantes para o chamado, acesso a documentação, base de conhecimento, download de atualizações, verificação de alertas relacionados à infraestrutura e compatibilidade de firmwares e softwares.
- 2.29. A solução deve permitir o provisionamento de armazenamento utilizando NFS/SMB ou armazenamento de objetos, por meio de tecnologia S3, para no mínimo 1 TiB, com pelo menos as seguintes características:
- 2.29.1. Para armazenamento de arquivos e objetos o SDS deverá permitir a otimização dos dados utilizando tecnologia erasure coding na camada de capacidade.
- 2.29.2. Permitir que usuários recuperem seus arquivos de maneira granular, sem necessidade de intervenção do administrador do SDS. Para o protocolo SMB a recuperação deverá ser realizada pela propriedade de Versões Prévias da pasta destino. Para o protocolo NFS, através da listagem do subdiretório escondido (snapshot).
- 2.29.3. Para segurança na estratégia de DevOps, a solução deverá suportar autenticação com criptografia do tráfego entre o client e o servidor de arquivos através de kerberos 5 p.
- 2.29.4. Suportar a integração com software de antivírus de terceiros através do protocolo ICAP (Internet Content Adaptation Protocol) para compartilhamento via SMB e permitir a varredura de arquivos em tempo real quando o arquivo é aberto, fechado ou modificado.
- 2.29.5. Deverá permitir a configuração de um ambiente de detecção avançada de intrusão (AIDE) que identifique desvios na configuração de segurança do File Server e restabeleça a configuração suportada sem necessidade de intervenção do administrador.
- 2.29.6. Habilitar encriptação em nível de pasta (SMB Encryption).
- 2.29.7. Suportar a organização de pastas compartilhadas entre diferentes servidores em um mesmo local ou geograficamente distantes através de um único "Single namespace", inserindo um diretório hierárquico unificado de modo a simplificar a integração com soluções existentes ou futuras através do protocolo DFS-N (DFS Namespaces).
- 2.29.8. Suportar autenticação via "Active Directory", "LDAP" e acesso não gerenciado a compartilhamento via NFSv4 e autenticação via LDAP e acesso não gerenciado via protocolo NFSv3.
- 2.29.9. Suportar acesso multiprotocolo a uma ou mais pastas, ou seja, ser capaz de prover acesso tanto via SMB quanto via NFS a um mesmo compartilhamento utilizando de protocolos como Windows ACLs (Access Control Lists) e Unix mode bits.
- 2.29.10. O armazenamento de Objetos deve possuir uma interface de API REST compatível com Amazon Web Services Simple Storage Service (AWS S3), capaz de lidar com petabytes de dados não estruturados e gerados por máquina, para casos de uso relacionados ao armazenamento para backup e retenção de longo prazo e armazenamento de dados para aplicativos nativos da nuvem usando APIs S3 padrão.
- 2.29.11. Permitir que os usuários da plataforma armazenem e gerenciem dados não estruturados em uma arquitetura resiliente e altamente escalável.

- 2.29.12. Permitir a gestão de objetos através da interface de gestão gráfica da solução de cloud e através de APIs REST compatíveis com S3, após autorização do administrador para que usuários e aplicativos possam acessar os buckets.
- 2.29.13. Permitir a configuração de serviços de diretórios, compatível com Microsoft Active Directory e OpenLDAP, para adicionar facilmente pessoas que devem ter acesso aos objetos.
- 2.29.14. Permitir o compartilhamento dos "buckets" com os usuários que possuem as chaves de acesso, assim como, permitir a delegação de permissões como escrita e leitura de acordo com o nível de acesso.
- 2.29.15. Permitir a listagem dos buckets compartilhados, identificando quais usuários possuem acesso a cada um deles.
- 2.29.16. Permitir o gerenciamento dos buckets e seus respectivos objetos usando APIs REST compatíveis com a solução de gerenciamento central do cluster ou S3 depois que um administrador autorizar os aplicativos e usuários a acessarem os buckets adequadamente.
- 2.29.17. Permitir o versionamento de múltiplas versões de um objeto dentro de um mesmo bucket.
- 2.29.18. Permitir a criação de um conjunto de regras para definir ações do ciclo de vida de um objeto, como permitir que um objeto se apague automaticamente depois de um determinado número de dias, meses ou anos, assim como, apagar determinada versão de um objeto após um determinado período de tempo.
- 2.29.19. Permitir a prevenção da deleção ou alteração de um objeto existente de acordo com um determinado período de retenção, utilizando de algoritmos de WORM (Write-Once-Read-Many).
- 2.29.20. A solução deverá possuir uma ferramenta para automatizar e orquestrar todos os procedimentos necessários para atualização dos firmwares e softwares relacionados com um assistente para elaborar todo o planejamento e sequenciamento dos procedimentos de atualização.
- 2.29.21. O software deve incorporar segurança em conformidade com padrões governamentais e internacionais de segurança e privacidade, NIST SP800-53, Common Criteria EAL2+, constar na lista de produtos aprovados pela rede de informação do Departamento de Defesa norte americano (DoDIN APL), além de permitir o emprego de configurações baseadas no Guia de Implementação Técnica de Segurança (STIG) da Agência de Sistemas de Informação do Departamento de Defesa dos EUA (DISA).
- 2.29.22. A solução de hiperconvergência contratada deve, através de software próprio ou de terceiros, prover as seguintes funções, para pelo menos 20 imagens de container:
- 2.29.23. Analisar, testar e reportar falhas de segurança em aplicações em Containers Docker como parte dos ativos a serem inspecionados;
Analisar imagens preparadas pelos desenvolvedores na esteira DevOps em busca de imagens com vulnerabilidades identificadas e malware residente no sistema de arquivos;
Integrar a esteira DevOps através de API, invocando o envio da imagem para análise em repositório próprio da solução ou utilizando scanner implementado em infraestrutura proprietária do órgão com a finalidade de evitar o envio de imagens e propriedade intelectual da contratante;
- 2.29.24. A console de administração destas funções deverá possuir controle de acesso no mínimo permitindo usuários com capacidade de somente visualizar as informações, e usuários com capacidade para efetuar análise das imagens;
- 2.29.25. Inventariar o sistema operacional de cada imagem analisada e suas vulnerabilidades encontradas;
- 2.29.26. Identificar containers que não foram analisados antes de sua implementação em produção;
- 2.29.27. Analisar as camadas (layers) de um container;
- 2.29.28. Identificar containers que tiveram mudanças de arquivos entre a análise e a sua implementação em produção;
- 2.29.29. Informar os CVEs para cada vulnerabilidade encontrada nos pacotes e bibliotecas residentes na imagem;
- 2.29.30. Deve ter a capacidade de testar automaticamente todas as imagens armazenadas, ou previamente testadas, sempre que uma nova vulnerabilidade for publicada e atualizada no banco de dados de vulnerabilidade da solução, sem qualquer tipo intervenção manual;
- 2.29.31. Inventariar os pacotes e bibliotecas e suas respectivas versões e listar as mesmas dentro do relatório de resultados de análise de cada imagem;

- 2.29.32. Fornecer scanner em formato Docker para implementação local e análise de imagens sem a necessidade de envio destas para repositório remoto, fora do ambiente da contratante;
- 2.29.33. Deve ser capaz de configurar políticas usando como condições: CVSS Score, CVEs específicos e Malware identificado;
- 2.29.34. Deve permitir a criação de políticas específicas por repositório;
- 2.29.35. Deve prover integração com as seguintes plataformas de integração contínua: Bamboo, CircleCI, Codeship, Distelli, Drone.io, Jenkins, Shippable, Solano Labs, Travis CI, Wrecker e Kubernetes.

3. Especificações Gerais

- 3.1. Os equipamentos dos itens 1 e 2 deverão ser ofertados com garantia do fabricante durante 60 meses, suporte 24x7 e reposição de peças até o próximo dia útil após a confirmação da necessidade de reposição de peças.
- 3.2. A subscrição dos softwares deverão ter suporte para 60 (sessenta) meses 24x7, com início de atendimento em até 1h (uma hora) após abertura de chamados críticos.
- 3.3. A contratada deverá fornecer todos componentes necessários para a conectividade dos itens 1 e 2, dentre eles: cabos, adaptadores, switches, etc.
- 3.4. Todas as conexões e equipamentos deverão ser redundantes e as portas dos equipamentos de rede deverão ser compatíveis com as portas dos itens 1 e 2, devendo operar em sua velocidade máxima, bem como a capacidade máxima de switching deverá suportar o tráfego de todas as portas em operação simultânea. O uplink com a rede atual deverá possuir, no mínimo, 80 Gbps.
- 3.5. A contratada deverá realizar a instalação física e migração de todo o ambiente atual para a nova solução contratada. Para isso, deverá possuir, pelo menos, um profissional certificado com o nível de certificação acima de profissional (profissional) do caminho de certificação do fabricante.
- 3.6. A contratada deverá realizar o treinamento dos produtos ofertados para pelo menos 8 pessoas com carga horária de 20 horas no formato remoto.

Brasília, 11 de junho de 2024.

80000.000073/2024-16

80000.000073/2024-16

5083285v1



Documento assinado eletronicamente por **Emerson Moreira de Moraes, Coordenador de Infraestrutura da Informação**, em 12/06/2024, às 13:05, com fundamento no art. 4º, § 3º, do Decreto nº 10.543, de 13 de novembro de 2020.



A autenticidade do documento pode ser conferida no site https://sei.mi.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **5127302** e o código CRC **C9F90157**.