Seu caminho para a resiliência com Veeam Kasten

Um roteiro para os seus primeiros 100 dias e além.

Este guia orienta administradores de TI na implantação, configuração e operacionalização do Veeam Kasten *for Kubernetes*. Seja instalado por meio do Helm ou do Marketplace, o processo de implantação foi projetado para ser rápido, seguro e acessível. Em 100 dias, você terá um ambiente de backup nativo para Kubernetes com exportações externas imutáveis, integrado aos seus conjuntos de ferramentas e aplicações, além de um manual de recuperação documentado.

Sua Jornada de 100 Dias

FASE 1 **Fundação** **Dias 1-14**	FASE 2 **Reforçar o Básico** **Dias 15-45**	FASE 3 **Otimizar e Reforçar** **Dias 46-75**	FASE 4 **Demonstrar Valor** **Dias 76-100**
M1: Dimensionamento e Planejamento	M4: Gerenciamento centralizado	M7: Integração de observabilidade	M10: Teste de recuperação
M2: Implantar Veeam Kasten	M5: Processamento com percepção de aplicações	M8: Resiliência aprimorada	M11: Documentação e relatórios
M3: Primeiros jobs de backup	M6: Melhores práticas para políticas	M9: Fechamento das lacunas de cobertura	M12: Higiene Operacional Contínua

Visão rápida do roadmap

Fase	Nome	Linha do tempo	Foco
FASE 1	Fundação	Dias 1-14	Planeje o ambiente, implante o Veeam Kasten e execute os primeiros jobs de backup
FASE 2	Reforçar o Básico	Dias 15-45	Gerenciamento centralizado, processamento com percepção de aplicações e melhores práticas de políticas.
FASE 3	Otimizar e Reforçar	Dias 46-75	Observabilidade, resiliência e DR, além de eliminar lacunas de cobertura.
FASE 4	Demonstrar Valor	Dias 76-100	Testes de recuperação, documentação e práticas de manutenção contínua.

Como usar este guia

Os dias são diretrizes, não prazos rígidos. Ambientes pequenos podem comprimir a Fase 1 para uma semana, e ambientes complexos podem estender a Fase 3.

Cada marco se baseia no anterior, portanto, recomenda-se seguir os passos em ordem.

Caixas de texto explicativo ao longo do guia destacam pontos de decisão, opções de arquitetura e armadilhas comuns que merecem atenção.

ìndice

FASE 1 • Dias 1-14

Fundação

Objetivo: infraestrutura dimensionada, implantada e primeiras cargas de trabalho protegidas.

Marco 1: Dimensionamento e Planejamento

Antes de implantar qualquer coisa, invista tempo no planejamento. A maioria dos desafios com a implantação de um ambiente estável e bem protegido pode ser evitada com a devida atenção a essa etapa.

Inventário de cargas de trabalho

- Documente a contagem total de cargas de trabalho e máquinas virtuais (VM), o espaço ocupado pelos dados (por exemplo, tamanho do volume/contagem de arquivos) e a taxa de alteração diária estimada.
- Identifique suas cargas de trabalho essenciais. Essas cargas de trabalho determinam suas metas de objetivo de ponto de recuperação (RPO) e objetivo de tempo de recuperação (RTO).
- Anote quaisquer bancos de dados e cargas de trabalho que possam se beneficiar do processamento com percepção de aplicações.

Planejamento de Dimensionamento e Implantação do Veeam Kasten

- O Veeam Kasten tem requisitos mínimos de sistema e os valores padrão geralmente são suficientes.
- Escolha o método de implantação, seja Marketplace/Operator (recomendado sempre que possível) ou Helm. É possível alterar o método de implantação após a instalação, caso seja necessário.
- Verifique se a sua versão do Kubernetes é compatível com a versão mais recente do Veeam Kasten. Se não for compatível, você terá que fazer upgrade primeiro ou recorrer a uma versão mais antiga.
- Determine se este ambiente está isolado. Se for o caso, talvez seja necessário enviar as imagens do Veeam Kasten para um registro local disponível offline por meio do marketplace do seu fornecedor, ou incluir nosso registro na lista de permissões.
- Planejar sua rede de backup isolando o tráfego de backup em uma VLAN dedicada é uma das melhores práticas de segurança, e isso é possível com Kubernetes dependendo do seu CNI.

Helm VS Marketplace

Helm: Este é o mais flexível e compatível com todas as distribuições do Kubernetes.

Marketplace/Operator: O ciclo de implantação e atualização é mais simples e oferece suporte aos mesmos parâmetros de personalização do Helm. Também é comumente usado com o Red Hat OpenShift.

O contraponto: Pode haver um atraso potencial no recebimento de novos lançamentos pelo Marketplace. As atualizações estão disponíveis imediatamente no Helm, mas os fornecedores do marketplace geralmente atrasam novos lançamentos por um ou mais dias para testes de validação.

Arquitetura de Storage para Cargas de Trabalho

- **Storage com capacidade de snapshot:** O Veeam Kasten é compatível com praticamente qualquer driver de storage CSI com suporte a snapshots, além de integrações diretas com storage.
- **Outros tipos de storage (por exemplo, NFS genérico, disco local, etc.):** O Veeam Kasten ainda pode proteger essas cargas de trabalho, mas a falta de recursos reais de snapshot afeta a confiabilidade e o desempenho dos backups. Recomendamos fortemente que você faça upgrade para volumes com recursos de snapshot, mas GSB ou NFS tar podem ser usados se você aceitar suas limitações inerentes.

Arquitetura de Storage de Backup: Visão Geral das Opções

Sua escolha de storage molda a resiliência e a disponibilidade dos seus Dados de backup. Aqui está uma visão geral dos prós e contras de cada tipo de storage de backup que você pode configurar como um perfil de local.

Veeam Kasten + Veeam Vault

Os snapshots são exportados para storage de objetos imutáveis, local externo e logicamente isolado por meio do Veeam Vault. Nenhuma configuração avançada ou manutenção é necessária.

Veeam Kasten + Veeam Backup & Replication Repository

Os snapshots são exportados para a infraestrutura gerenciada do Veeam Backup & Replication, incluindo Veeam Hardened Repositories e Scale-out Backup Repositories (SOBRs). O modo de bloco é necessário. **Nota:** Versões anteriores à 9.x também exigem um pequeno perfil de local adicional (Vault/Object/NFS/CIFS) para metadados.

Veeam Kasten + Armazenamento de Objetos

Os snapshots são exportados para um storage de objetos (por exemplo, S3, nuvem), que deve ser configurado para ser externo e imutável.

Veeam Kasten + NFS/CIFS

Snapshots exportados diretamente para NFS/CIFS geralmente não oferecem imutabilidade, mesmo em dispositivos compatíveis com WORM, pois seria necessário versionamento para funcionar. Embora essa opção seja totalmente suportada, ela não é recomendada, a menos que você também tenha cópias ou duplicações imutáveis em um local externo.

Veeam Kasten + múltiplos perfis de localização

Os snapshots são exportados para dois ou mais locais. Se projetado corretamente, usando pelo menos uma opção imutável, esse pode ser o caminho mais resiliente. **Nota:** Versões anteriores à 9.x requerem várias Políticas, usando 1 Perfil de Local por Política.

Modos de Storage Determinam Recursos

Dependendo do seu tipo de storage, você pode ter as seguintes opções disponíveis:

Modo de volume: Arquivo ou Bloco. Ambos são compatíveis com o Veeam Kasten (por exemplo, Ceph FS ou RBD).

Modo de Exportação: Arquivo ou Bloco. Ambos são possíveis com Veeam Kasten.

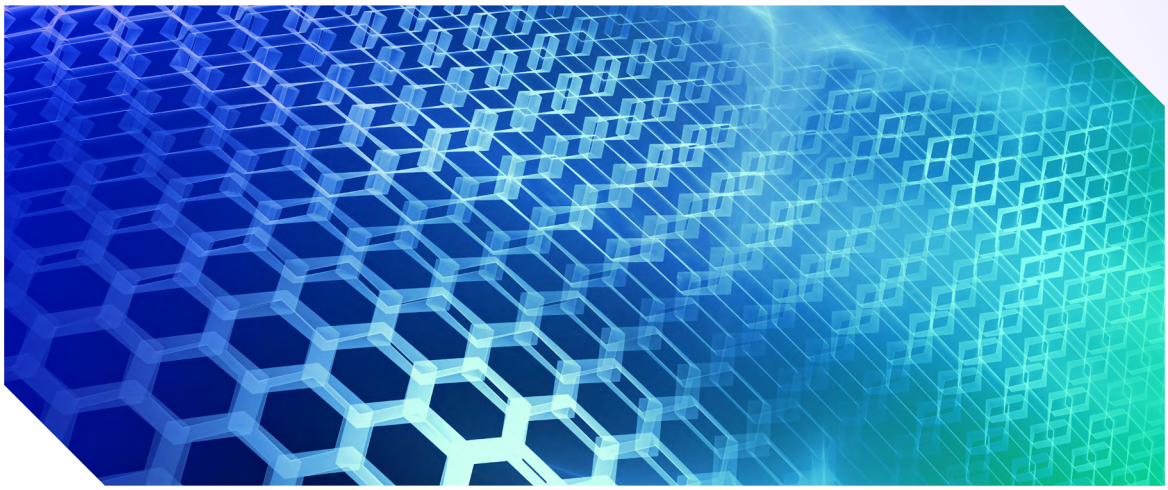
Se um volume estiver no modo de bloco, talvez seja possível exportar seus snapshots no modo de bloco. Isso oferece recursos especiais, como CBT (quando disponível) e exportações para um repositório do Veeam Backup & Replication.

Usando o Veeam Backup & Replication + Veeam Infrastructure Appliance (VIA) como repositório seguro

Para aqueles que não possuem storage imutável existente, integrar o Veeam Kasten com o Veeam Backup & Replication e implantar VIA pode ser um caminho razoável para alcançar a imutabilidade local.

Um repositório seguro fornece backups locais imutáveis, o que significa que o ransomware não pode criptografar ou excluir esses backups durante o período de retenção. O SO é protegido contra acesso não autorizado e idealmente deve ser executado em um servidor físico protegido, em vez de uma VM.

Tradicionalmente, um repositório seguro exige a instalação manual e o endurecimento de uma distribuição Linux. O VIA remove totalmente essa barreira, pois já é pré-endurecido e é implantado via ISO inicializável. Além disso, ele pode ser implantado manualmente em hardware compatível ou adquirido de um fornecedor na forma de um appliance certificado.



Marco 2: Implantar o Veeam Kasten

Implantar o Veeam Kasten

- Use ferramenta de verificação prévia para verificar se os requisitos são atendidos (opcional).
- Método Marketplace/operador: Consulte as instruções aqui.
- Método Helm: Consulte as instruções aqui.

Acesso ao painel e integração de autenticação

- Para acessar o painel externamente, adicione uma Entrada ou uma rota ao Veeam Kasten.
- É uma das melhores práticas integrar com o seu provedor de autenticação de distribuição (por exemplo, OpenShift Auth), mas outras opções, como o LDAP direto, também são possíveis.
- Quando o painel da Veeam Kasten estiver visível, você pode seguir as etapas abaixo.

Conecte a Infraestrutura ao Veeam Kasten

- Se aplicável, (vSphere/nuvem/outros) adicione um Perfil de Infraestrutura para integração direta com storage.
- Adicione um perfil de local para definir o destino do backup.

Marco 3: Primeiros trabalhos de backup

Backups em ambientes Kubernetes

Os storage snapshots são recursos avançados compreendidos pelo Kubernetes, que pode gerenciá-los de forma nativa, desde que sejam compatíveis com o provisionador de storage utilizado.

Veeam Kasten utiliza esses recursos ou integração direta para acionar snapshots que residem localmente no dispositivo de storage. O Veeam Kasten pode então usar esses snapshots para exportar dados de forma confiável para um perfil de local externo (como NFS, S3, repositório VBR, Vault, etc.).

Esse método permite o máximo de velocidade e consistência, ao mesmo tempo que utiliza recursos e APIs nativos do Kubernetes para garantir a máxima compatibilidade.

O que é necessário para começar

Veeam Kasten, sendo uma aplicação nativa do Kubernetes, requer que o usuário responsável pela instalação tenha acesso ao kubectl no ambiente de destino, privilégios de administrador do cluster e, idealmente, acesso à interface de gerenciamento da sua distribuição, se houver.

Dica: Se você encontrar algum erro, soluções podem ser encontradas em nossos sites da Comunidade e da KB.

- Saiba mais sobre como proteger VMs do KubeVirt, se aplicável ao seu ambiente.
- Crie sua primeira política de backup e configure o perfil de local como destino.
- Defina uma política de retenção adequada para começar: 1 snapshot local diário, com exportações para o perfil de local configuradas para retenção de 1 diária, 4 semanais e 3 mensais.
- Agende o trabalho para ser executado fora do horário de pico e certifique-se de que ele não conflite com outras janelas de manutenção.
- Execute o trabalho manualmente na primeira execução e monitore-o até a conclusão.
- Confirme que o trabalho seja concluído sem avisos ou erros antes de prosseguir para a Fase 2.

Seu primeiro teste de restauração: não deixe de realizar esta etapa

Antes de passar para a fase 2, realize uma restauração em uma aplicação não crítica para confirmar a recuperabilidade.

Você não está protegido até verificar que pode restaurar. Isso leva apenas alguns minutos e pode evitar dias de problemas posteriormente.

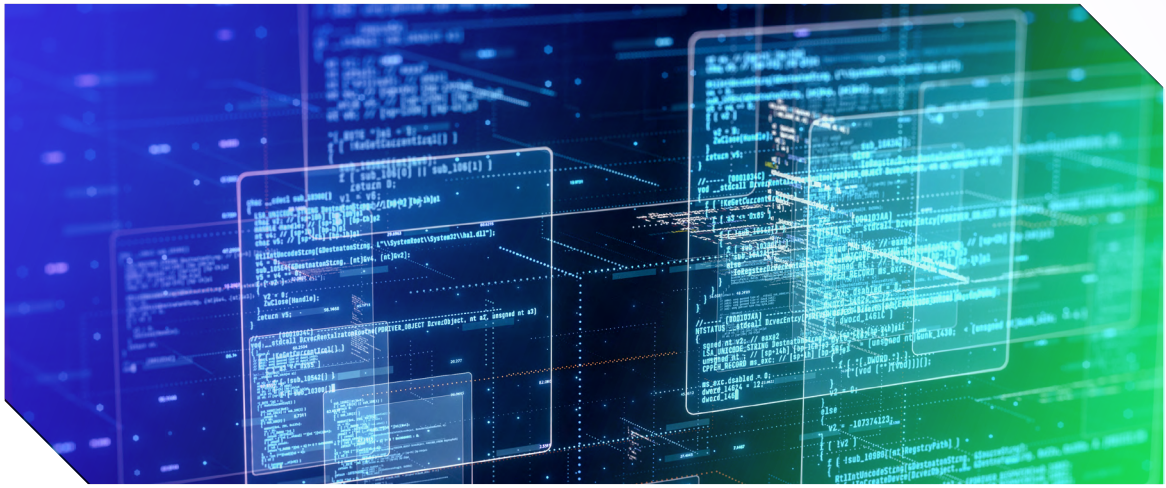
Local VS Exportação

Tenha em mente que os snapshots permanecem armazenados apenas no dispositivo de storage local. Isso significa:

- Eles não são um backup real.
- Quanto mais snapshots locais forem retidos, mais storage primário será consumido.

Portanto, é importante exportar os snapshots para um Perfil de Local, que pode ter uma política de retenção configurada independentemente.

Ao exportar snapshots, todos os dados são automaticamente deduplicados, comprimidos, criptografados e salvos de forma incremental.



FASE 2 • Dias 15-45

Fortaleça o básico

Objetivo: proteção consistente, cópia em local externo e visibilidade em todo o seu ambiente.

Marco 4: Gerenciamento Centralizado (MCM)

Multi-Cluster Manager (MCM) permite visibilidade e gerenciamento centralizados de múltiplos clusters. Cada cluster terá o Veeam Kasten instalado para proteger as cargas de trabalho, e as instâncias podem ser conectadas entre si.

- Depois que outro cluster executando o Veeam Kasten tiver sido implantado, promova uma instância do Kasten para Primária e use um Token de junção para vinculá-los (instruções). Garanta que certificados autoassinados sejam confiáveis para evitar erros.
- Veja todos os clusters conectados pelo painel MCM.
- Defina políticas globais e perfis globais se desejar ter uma configuração consistente distribuída por todo o ambiente.
- Adicione sua chave de licença corporativa ao cluster MCM primário. As licenças serão distribuídas automaticamente para todos os outros clusters, sem necessidade de configuração adicional.

Marco 5: Processamento com percepção de aplicações

O processamento com percepção de aplicações por meio dos Kanister Blueprints assegura que backups consistentes em caso de desastre sejam consistentes com as aplicações ou exportados de forma lógica. Isso é crítico para bancos de dados como PostgreSQL, MongoDB, MySQL, Elastic e outros.

- Discuta os requisitos e o acesso da aplicação com a equipe responsável pela aplicação.
- Encontre exemplos de Blueprints pré-criados que você pode personalizar ou crie os seus próprios.
- Adicione o Blueprint ao Veeam Kasten.
- Associe o Blueprint às cargas de trabalho manualmente ou criando um Blueprint Binding.
- Teste um backup e uma restauração usando seu Blueprint para validar a recuperação completa da aplicação.

Tipos de backups

Com controle de falhas (padrão): esse tipo de backup registra todo o sistema de arquivos em um instante específico, geralmente por meio de snapshots fornecidos pelo provedor de storage. Isso é mais consistente com os dados do que a cópia de arquivos básica, mas gravações em transmissão ou transações não confirmadas ainda podem ser perdidas.

Consistente com aplicações: Este tipo de backup normalmente coloca a aplicação em estado de pausa brevemente, utilizando as ferramentas nativas da aplicação para garantir que tudo seja escrito no volume antes da criação do snapshot.

Lógico: Este tipo de backup utiliza as ferramentas nativas da aplicação para gerar um dump lógico ou exportar seus dados como um arquivo. Isso geralmente é transferido para um local externo, como S3, em vez do próprio volume.

Blueprints são avançados e infinitamente flexíveis. Além disso, com sua natureza de código aberto, você pode criar um para qualquer aplicação ou fluxo de trabalho, caso não exista.

Marco 6: Melhores Práticas de Políticas

Nesta etapa, você criará trabalhos adicionais para proteger todas as suas cargas de trabalho e aplicará configurações avançadas para assegurar a confiabilidade delas.

Melhores práticas (para a maioria dos cenários)

- Use vários trabalhos com rótulos para selecionar aplicações, em vez de uma política curinga que protege tudo.
- Use políticas baseadas em VM em vez de baseadas em namespace ao proteger VMs KubeVirt.
- Se você deseja fazer backup de recursos com escopo de cluster, crie uma política separada para apenas esses backups.
- Defina uma janela de backup para garantir que as cargas de trabalho de produção não sejam afetadas durante horas críticas.
- É uma boa ideia agendar os trabalhos com agendamento escalonado para melhorar o desempenho.
- Configurar proteção de backup imutável.
- Exclusões / Filtros de recursos se necessário.
- (Opcional) Recursos globais, predefinições de políticas

Outras Dicas

Para trabalhos executados manualmente, a menos que um tempo de expiração seja especificado, quaisquer artefatos precisarão ser removidos manualmente.

Mesmo que o trabalho tenha sido configurado usando a hora local, todos os horários são convertidos em UTC e as agendas de políticas não são alteradas para o horário de verão.

Verifique seus cálculos! O cálculo de retenção nem sempre é simples. Por exemplo, se forem mantidos 24 snapshots realizados a cada 15 minutos, o período de retenção será de apenas 6 horas, e não de 24 horas.

FASE 3 • Dias 46-75

Otimizar e fortalecer

Objetivo: Eliminar lacunas de proteção, aprimorar RTO/RPO e aumentar a visibilidade.

Marco 7: Integração de observabilidade

- Habilite a integração do Red Hat ACM Observability, se aplicável.
- Exportar métricas para sistemas de monitoramento externos (por exemplo, Grafana, Datadog, Thanos, etc.).
- Crie alertas e painéis em seus sistemas de monitoramento (exemplo de Grafana).
- Habilite a geração de relatórios.

Marco 8: Resiliência aprimorada e DR

Ter um backup de todas as cargas de trabalho também deve abranger o backup do próprio Veeam Kasten, o que pode ser realizado com o Kasten Disaster Recovery (KDR). Isso não deve ser confundido com ter um ambiente de DR ou um plano de DR, todos os quais devem ser considerados com base na resiliência necessária.

KDR (backup do seu catálogo do Veeam Kasten)

- Ative Kasten DR: Isso salva o catálogo de backup do Veeam Kasten, permitindo que restaurações sejam possíveis mesmo que a instalação do Kasten não esteja mais acessível. Isso é importante, pois os arquivos de backup do Veeam Kasten não são independentes e requerem o catálogo e a chave de criptografia para serem restaurados.
- Configure o Kasten DR para "Exportar snapshots locais do catálogo" e salve as seguintes informações em um local seguro: passphrase (frase-secreta), ID do cluster, detalhes do perfil de local do KDR e credenciais.

DR para suas cargas de trabalho

- Determine o nível de resiliência necessário com base nos RTOs/RPOs desejados.
- Se um RTO/RPO de 1+ dias for aceitável, ter apenas backups e reconstruir o ambiente conforme necessário pode ser uma solução razoável.
- Se os RTOs/RPOs precisarem ser medidos em horas ou minutos, é necessário ter cuidado especial ao elaborar um plano. Veja alguns exemplos abaixo.

Exemplos de configurações de DR (conforme a necessidade de RTO/RPO)

- **Aplicação Desprotegida:** sem pontos de restauração (ou seja, sem snapshots locais ou exportações).

  Resultado: nenhuma recuperação possível.

- **Somente exportação:** as exportações do KDR e os pontos de restauração exportados estão disponíveis em um perfil de local externo.

  Resultado: Para recuperar, primeiro recrie um ambiente Kubernetes, instale o Veeam Kasten, restaure o catálogo do Kasten e depois restaure as aplicações a partir dos pontos de restauração exportados.

- **Ambiente de DR + Importação:** Veeam Kasten está instalado e uma Política de Importação é executada regularmente para importar os pontos de restauração para um catálogo local.

  Resultado: Os pontos de restauração ficam visíveis em um local secundário e estão prontos para serem restaurados. Recursos mínimos são consumidos até que sejam necessários.

- **Ambiente de DR + Importação e Restauração, escalado para zero:** Veeam Kasten está instalada, a Política de Importação e Restauração executa regularmente para importar os pontos de restauração ao catálogo local e então restaurar aplicações no ambiente Kubernetes. As aplicações são restauradas posteriormente, porém com Transformações que definem as réplicas como 0 em todas as cargas de trabalho.

  Resultado: As aplicações são restauradas no Kubernetes (via pods, PVs, tudo selecionado). No entanto, com as réplicas definidas como 0, apenas recursos mínimos são utilizados até que sejam necessários, com exceção do armazenamento.

- **Ambiente de DR + Importação e Restauração, completo:** Veeam Kasten está instalado, a política de Importação e Restauração é executada regularmente para importar os pontos de restauração para um catálogo local e depois restaurar as aplicações para o ambiente Kubernetes.

  Resultado: Aplicações são restauradas no Kubernetes (via pods, PVs, tudo selecionado), funcionando exatamente como estavam na produção e prontas para serem totalmente utilizadas.

Planejamento para desastres

O Veeam Kasten é independente de distribuição, ou seja, pode restaurar de e para qualquer distribuição do Kubernetes, até mesmo entre plataformas totalmente distintas, como de Tanzu para Azure. Porém, as restaurações exigem que exista um ambiente funcional do Kubernetes para serem executadas; o Kasten não pode se auto-inicializar. Certifique-se de criar um plano de desastre adequado para que você esteja pronto caso haja um incidente e teste regularmente se seu plano está atingindo seus objetivos.

Marco 9: Ajuste Fino

- **Revise o painel do Veeam Kasten:** Trate todas as cargas de trabalho desprotegidas antes de fazer qualquer outro ajuste.
- **Revise os agendamentos de tarefas em busca de conflitos:** Escalone os horários de início para evitar a contenção de recursos.
- Confirme se todas as tarefas estão sendo concluídas dentro da sua janela de backup definida.
- **Valide a conformidade com o RPO:** Todas as cargas de trabalho essenciais estão gerando pontos de restauração dentro do prazo de recuperação definido?
- Confirme se todas as cargas de trabalho estão exportando para pelo menos um local imutável.
- Habilitar coleta de lixo para remover ações obsoletas pode ajudar no desempenho do catálogo.
- Teste seu processo de upgrade! Novas versões do Veeam Kasten são lançadas aproximadamente a cada duas semanas.

FASE 4 • Dias 76-100

Demonstre Valor e Operacionalize

Objetivo: Verificar a recuperabilidade, estabelecer boas práticas contínuas e demonstrar o ROI.

Marco 10: Testes de recuperação

O único backup que importa é aquele a partir do qual você pode restaurar. A fase 4 é onde você comprova, com evidências documentadas, que seu ambiente está cumprindo seus compromissos de RTO e RPO.

Testes de restauração granular e completa

- Teste uma restauração completa de um namespace ou uma Restauração de VM a partir de uma exportação. Simule uma perda total on-premises para validar sua cópia externa.
- Teste de recuperação de item de aplicação: Restaure um banco de dados e execute consultas para verificar se os dados estão íntegros.
- Teste a restauração no nível do arquivo (se desejar): recupere arquivos individuais de uma exportação para um local de teste.
- Teste o seu plano de DR completo de ponta a ponta, registre quaisquer problemas para aprimorar e documente extensivamente o processo de forma a garantir que o seu plano de DR e o acesso a ele estejam disponíveis.
- Registre os tempos de recuperação reais e compare com suas metas de RTO. Documente os resultados.

Melhores Práticas para Testes de Recuperação

Sempre restaure para um ambiente não produtivo e nunca sobrescreva cargas de trabalho em produção durante um teste.

Documente o que foi restaurado, de qual ponto de restauração, para qual destino e quanto tempo levou.

Esses resultados são prova da recuperabilidade. Retenha-os para revisões de conformidade, auditorias e relatórios gerenciais.

Além disso, ao restaurar no mesmo ambiente, mesmo para namespaces diferentes, esteja ciente de que determinados recursos (especialmente serviços de rede) podem entrar em conflito. Certifique-se de revisar sua configuração antes de restaurar, restaurar para um ambiente diferente e/ou usar Transforms para evitar conflitos.

Restaurar em Diferentes Ambientes

Se estiver restaurando de/para diferentes sites, distribuições Kubernetes, plataformas ou outros ambientes, Transforms podem ser úteis para modificar sua configuração de forma transparente durante a restauração. Por exemplo, se você estiver alterando caminhos de rede de Production para DR ou alterando classes de storage. Não são necessárias alterações manuais para que suas restaurações sejam executadas imediatamente com uma configuração modificada ou em um novo ambiente.

Marco 11: Documentação e Relatórios

- Habilite a geração de relatórios, se ainda não tiver sido feito.
- Documente sua arquitetura final de backup, incluindo lista de políticas, locais de exportação, agendamentos e políticas de retenção.
- Analise o consumo de storage do Veeam Vault e confirme se a utilização está alinhada com o orçamento esperado.
- Arquive os resultados dos testes de recuperação junto com a documentação de arquitetura.

Marco 12: Estabeleça uma cadência de higiene contínua

Até o dia 100, seu ambiente deve estar estável e totalmente documentado. Esses hábitos mantêm as coisas assim:

- **Semanalmente:** Revise o painel da Veeam Kasten e investigue quaisquer tarefas com falha ou alerta antes que elas se acumulem.
- **Mensalmente:** Revise as versões recentes da Kasten e atualize regularmente.
- **Trimestral:** Realize um teste de recuperação documentado e faça a rotação entre diferentes tipos de carga de trabalho a cada trimestre.
- **Anualmente:** Reveja sua arquitetura de backup em relação aos requisitos atuais de negócios.
- **Antes da renovação:** Analise o uso de licenciamento no seu Painel da Kasten (por exemplo, total via MCM ou em cada cluster individualmente) para confirmar que você está dentro do licenciamento contratado.

Próximos passos

Pronto para mais?

- Acesse a Veeam University
- Conheça histórias de sucesso de colegas
- Fale com a equipe de Atendimento ao Cliente
- Compartilhe sua história sobre resiliência de dados com a Veeam

Apêndice: Referência rápida

Componentes-Chave: Integração Veeam

- **Veeam Software Appliance (VSA):** Um appliance pré-endurecido com o Veeam Backup & Replication pré-instalado. Implante em formato OVA (VM) ou ISO (físico). Pode atuar como um repositório imutável limitado ou funcionar com outros appliances ou storage de backup, incluindo VIAs dedicadas.
- **Veeam Infraestrutura Appliance (VIA):** Um appliance pré-hardenizado implantado como um repositório seguro dedicado ou em outros papéis. Fornece imutabilidade local sem necessidade de conhecimento especializado em Linux. Um papel por appliance.
- **Veeam Backup & Replication:** Mecanismo principal de backup, hospedado no VSA. Gerencia tarefas, repositórios, proxies e operações de recuperação.
- **Scale-Out Backup Repository:** Estrutura lógica que combina um Performance Tier local (por exemplo, VIA) e um Capacity Tier (por exemplo, Vault/S3/NFS) em um único destino de backup.
- **Veeam Vault:** storage de objetos em nuvem imutável para cópias fora do local. É gerenciado pela Veeam, portanto sem necessidade de uma conta de nuvem separada.

Termos-chave

- **RPO:** Perda de dados máxima aceitável, medida em tempo. Determina a frequência do agendamento de backups.
- **RTO:** Tempo máximo de inatividade aceitável antes que uma carga de trabalho precise ser recuperada.
- **Imutabilidade:** Dados de backup que não podem ser modificados ou excluídos por um período de retenção definido. Protege contra a criptografia de arquivos de backup por ransomware.
- **Veeam Hardened Repository:** Um repositório de backup baseado em Linux com imutabilidade imposta no nível do SO. Fornecido pronto para uso pela VIA, sem necessidade de administração Linux.
- **KubeVirt:** Um projeto de código aberto que permite ao Kubernetes executar e gerenciar máquinas virtuais (VMs) juntamente com cargas de trabalho em contêineres. Isso permite que as VMs sejam executadas em plataformas Kubernetes, como OpenShift Virtualization e SUSE Harvester, que podem ser protegidas pelo Veeam Kasten.
- **processamento com percepção de aplicações:** Processamento que cria pontos de Backup consistente com aplicação, algo que o Veeam Kasten pode realizar utilizando Blueprints.
- **Blueprint:** Kanister Blueprints são um mecanismo de código aberto para descrever tarefas personalizadas de gerenciamento de dados em nível de aplicação no Kubernetes.

Recursos úteis

- Veeam Help Center
- Portal do Cliente Veeam (downloads)
- Veeam Community Forums
- Artigos da KB da Veeam
- Documentos do Veeam Kasten
- Documentação dos Blueprints do Kanister

Sobre a Veeam Software

A Veeam é a empresa líder em confiança de dados e IA, especializada em ajudar organizações a garantir que seus dados e IA sejam totalmente compreendidos, protegidos e resilientes, possibilitando a expansão segura de IA em escala. Como líder de mercado em resiliência de dados e gestão da postura de segurança de dados, a Veeam foi desenvolvida para a convergência de identidade, dados, segurança e riscos de IA.

Com sede em Seattle e escritórios em mais de 30 países, a Veeam protege mais de 550.000 clientes em todo o mundo, incluindo 82% das empresas da Fortune 500.

SAIBA MAIS em www.veeam.com ou siga a Veeam no LinkedIn @veeam-software e no X @veeam.