Veeam Data Platform

Primeiros 100 dias

Guia Prático de Integração para Administradores de TI

Índice

1. Sumário executivo

A Veeam Data Platform é a base da sua organização para resiliência contra ransomware e continuidade operacional. Este guia foi elaborado para ajudar as equipes de TI a operacionalizar e amadurecer seu ambiente de forma estruturada. Embora utilizemos o termo "primeiros 100 dias", isso é apenas uma metáfora para uma linha do tempo. Cada organização é diferente e pode avançar em ritmos variados, mas o objetivo é o mesmo: evoluir da configuração inicial para um estado mais seguro, resiliente e preparado para recuperação. Ele é organizado em torno de marcos práticos e resultados recomendados, em vez de exigências rígidas de implementação, permitindo que você se concentre nas etapas mais relevantes para o seu ambiente e edição.

2. Para quem é este guia?

Este guia destina-se a **administradores de TI** que estão implantando, configurando e operacionalizando a Veeam Data Platform. Pressupõe que você tenha familiaridade com infraestrutura virtualizada (por exemplo, VMware vSphere, Microsoft Hyper-V ou qualquer outro hipervisor suportado pelo Veeam Backup & Replication) e conhecimentos básicos de administração do Windows Server. Não é necessário ter especialização em Linux.

Ela também serve como referência compartilhada para **gerentes de TI** que estão rastreando escopo e cronogramas, partes interessadas em segurança e conformidade que estão validando a postura de hardening, e equipes de liderança ou de compras ao definir o que representa o sucesso no Dia 100.

3. O Que Você Alcançará Até o Dia 100

Até o Dia 100, você terá um ambiente estável, fortalecido e com capacidade comprovada de recuperação, que reduz o risco de paralisação e permite uma recuperação rápida e confiante, não importa o que aconteça.

Cada cliente deve ser capaz de confirmar que os seguintes pontos de verificação foram atendidos:

- **Implantado:** O Veeam Backup & Replication está em execução, conectado e dimensionado para atender às janelas de backup.
- **Protegido:** Cargas de trabalho prioritárias recebem backup com sucesso em um cronograma definido.
- **Endurecido:** Imutabilidade está implementada localmente e/ou externamente para defender contra ransomware.
- **Recuperação verificável:** Os testes de restauração estão concluídos, documentados e alinhados com as metas de objetivo de tempo de recuperação e objetivo de ponto de recuperação (RTO e RPO).
- **Operacionalizado:** Monitoramento, alertas, relatórios e runbooks de recuperação estão implementados e sob responsabilidade definida.

4. Visão rápida do roadmap

Este Guia está estruturado em quatro fases sequenciais, cada uma voltada para alcançar os resultados do Dia 100:

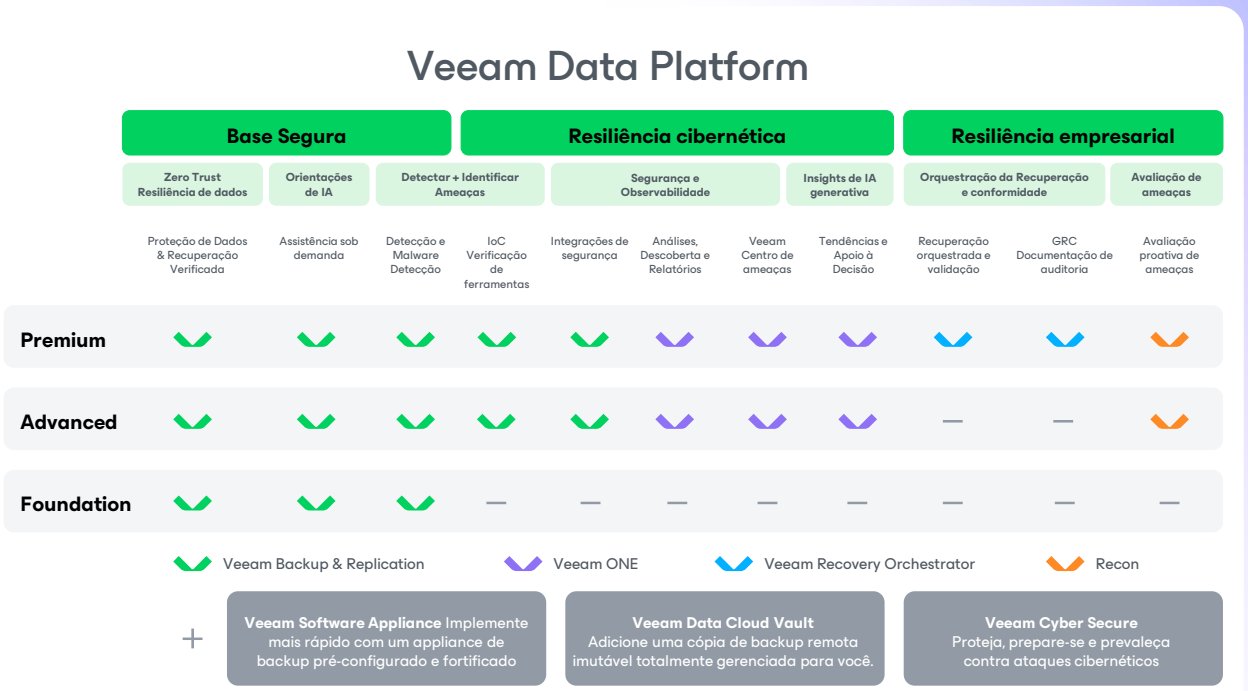
Fase	Nome	Linha do tempo	Foco
FASE 1	Foundation	Dias 1—14	Dimensione o ambiente, implante o Veeam Software Appliance (e o Veeam Infrastructure Appliance, se aplicável), execute os primeiros jobs de backup, prepare-se para o Veeam Recovery Orchestrator.
FASE 2	Otimizar	Dias 15—45	Processamento com percepção de aplicações, Tarefas de cópia de backup, camada off-site do Veeam Data Cloud Vault e configuração do Veeam Recovery Orchestrator (Premium).
FASE 3	Resiliência de dados e resiliência dos negócios	Dias 46—75	Fechamento de lacunas de cobertura, habilitação do Recon, prontidão contra ransomware, ajuste e criação de planos de orquestração (Premium).
FASE 4	Provar o valor	Dias 76—100	Testes orquestrados de recuperação, geração de relatórios, arquitetura de documentos e higiene contínua.

Como usar este guia

- Siga os marcos em ordem. Pular etapas, especialmente para a configuração do Scale-Out Backup Repository (SOBR) ou do Vault, antes que seus repositórios e jobs locais estejam estáveis, cria lacunas que normalmente aparecem durante uma restauração real.
- O cronograma é flexível. Os dias são diretrizes, não prazos rígidos. Ambientes menores podem concluir a Fase 1 em menos de uma semana. Ambientes mais complexos podem demandar mais tempo em fases posteriores.
- Use os pontos de decisão. Quando surgirem opções de arquitetura (p. ex., caminho de implantação ou estratégia de repositório), pause, alinhe as partes interessadas e documente sua decisão antes de prosseguir.
- Pule o que não se aplica, mas registre o motivo. Se a sua edição não incluir o Veeam ONE ou o Veeam Recovery Orchestrator, esses marcos serão claramente identificados. Da mesma forma, as etapas do Veeam Software Appliance e do Veeam Vault são opcionais e relevantes somente se esses módulos fizerem parte da sua implantação.

Visão geral da Veeam Data Platform

Antes de iniciarmos a implantação, vamos começar com uma breve recapitulação do que inclui a sua Veeam Data Platform. A Veeam Data Platform está disponível em três edições, cada uma baseada na anterior:



Consulte o apêndice para obter descrições de todos os componentes: "Apêndice: Referência rápida. Principais componentes".

Reserve um momento para confirmar sua edição.

Antes de prosseguir, confirme sua edição e faça um levantamento completo do que está incluído. Em proteção de dados, recursos não utilizados não são apenas valor desperdiçado — são lacunas esperando para serem expostas.

Além disso, os seguintes módulos estão disponíveis em todas as edições:

- **Veeam Software Appliance:** Uma plataforma de implantação pré-hardenizada, sem Windows, que simplifica a configuração da infraestrutura e fortalece a postura de segurança. Não é necessário ter conhecimento de Linux.
- **Veeam Vault:** Storage de backup imutável e externo, fornecido como um serviço para proteger seus dados contra ransomware e exclusão acidental.
- **Veeam Agents:** Os Veeam Agents são agentes de software que oferecem backup e recuperação no nível da imagem com qualidade Veeam para servidores físicos, endpoints e plataformas de máquinas virtuais (VM) não suportadas, gerenciados de forma centralizada a partir do console do Veeam Backup & Replication.

O caminho para a resiliência começa aqui.

Ao longo dos próximos 100 dias, você passará da implantação para um ambiente totalmente endurecido, verificável e recuperável, passo a passo, sem adivinhação.

FASE 1 **Foundation** **Dias 1—14**	FASE 2 **Otimizar** **Dias 15—45**	FASE 3 **Resiliência de Dados e Resiliência dos Negócios** **Dias 46—75**	FASE 4 **Provar o valor** **Dias 76—100**
M1: Dimensionamento e Planejamento	M4: Processamento com percepção de aplicações	M7: Fechamento das lacunas de cobertura	M10: Teste de recuperação
M2: Implantação do Veeam Software Appliance e da infraestrutura	M5: Cópia de backup, SOBR e Vault	M8: Prontidão contra ransomware	M11: Relatórios e Documentação
M3: Primeiros jobs de backup	M6: Monitoramento, Geração de Alertas e Configuração do Orchestrator	M9: Ajuste de Desempenho e Planos de Orquestração	M12: Higiene Operacional Contínua

FASE 1 • Dias 1—14

Foundation

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

Marco 1: Dimensionamento e Planejamento

Antes de implantar qualquer coisa, invista tempo no dimensionamento. O subdimensionamento da infraestrutura é a causa mais comum de janelas de backup lentas e RPOs perdidos nos primeiros 100 dias.

Inventário de cargas de trabalho

- Documente sua contagem total de VMs e cargas de trabalho, o espaço ocupado (total provisionado versus usado) e a taxa de alteração diária estimada.
- Identifique as cargas de trabalho essenciais, pois são elas que determinam seus objetivos de RPO e RTO.
- Identifique todas as cargas de trabalho físicas (por exemplo, servidores Windows/Linux) que necessitam do uso de Veeam Agents.

Dimensionamento do Veeam Software Appliance

- O Veeam Software Appliance já possui o Veeam Backup & Replication pré-instalado, então sua principal decisão de dimensionamento é escolher o host em que ele será executado.
- Mínimo para pequenas e médias empresas (PMEs): 8 vCPU / 16 GB de RAM (recomendado 500 MB de RAM para cada tarefa concorrente).
- Utilize a Calculadora de Dimensionamento da Veeam (calculator.veeam.com) para validar os requisitos de recursos para a quantidade de cargas de trabalho e o espaço ocupado dos dados.
- Escolha seu formato de implantação: um OVA para VMware vSphere ou um ISO para servidores físicos e outros hipervisores. De qualquer forma, não é necessária experiência com Linux.

Arquitetura de Storage: Escolha Seu Caminho

Sua escolha de storage neste estágio molda o restante das Fases 1 e 2. Há três caminhos recomendados para PMEs:

Caminho A: Veeam Software Appliance + Veeam Infrastructure Appliance como um Veeam repositório seguro + Vault: Esta é a configuração recomendada. Esse caminho oferece um repositório local imutável sem necessidade de conhecimento de Linux, além de cópias imutáveis remotas e logicamente isoladas por meio do Vault.

Caminho A: Por que usar um repositório seguro da Veeam fornecido via Veeam Infrastructure Appliance?

Um repositório seguro da Veeam fornece backups locais imutáveis. Isso significa que o ransomware não pode criptografar ou excluir os backups durante o período de retenção.

Tradicionalmente, um repositório Linux imutável requer um servidor Linux dedicado e fortalecimento manual do SO. O Veeam Infrastructure Appliance elimina inteiramente essa barreira. Ele vem pré-configurado com hardening, pode ser implantado a partir de um OVA ou ISO e não requer conhecimento em Linux para instalação ou administração.

O Veeam Infrastructure Appliance é um appliance de função única. Cada instância funciona como um repositório seguro da Veeam ou um proxy de backup. Para PMEs sem um administrador Linux dedicado ou storage imutável existente, um repositório seguro fornecido pelo Veeam Infrastructure Appliance é o caminho recomendado para imutabilidade local.

Para máxima proteção, implante o Veeam Infrastructure Appliance em hardware físico. Executar o Veeam Infrastructure Appliance como um appliance virtual ainda herda a superfície de ataque do hipervisor. A imutabilidade em nível de sistema de arquivos protege os arquivos de backup contra ataques dentro do SO, mas um administrador do hipervisor ainda pode excluir VMs diretamente, mesmo que os arquivos estejam imutáveis.

Caminho B: Veeam Software Appliance + Veeam Data Cloud Vault: O Veeam Backup & Replication escreve os backups diretamente no repositório local do Veeam Software Appliance e mantém uma cópia remota no Veeam Vault. Isso é ideal para microPMEs, filiais ou clientes que desejam minimizar o gerenciamento de storage local, além de cópias imutáveis em local externo e logicamente isoladas via Vault. Tenha em mente que, se o Veeam Software Appliance for implementado em uma infraestrutura virtual, ele não substitui adequadamente a imutabilidade no local.

Caminho B: Por que Veeam Software Appliance + Vault?

O caminho B reduz ao mínimo a administração do storage. O Veeam Backup & Replication grava os backups em um repositório local no próprio Veeam Software Appliance e, em seguida, uma tarefa de cópia de backup os replica externamente para o Vault.

O storage local do Veeam Software Appliance é imutável por padrão, então o Caminho B ainda oferece proteção no local contra ransomware. Não é um repositório seguro da Veeam formal no sentido de produto, então o caminho A continua sendo a escolha mais sólida quando você tem hardware para dedicar ao Veeam Appliance de infraestrutura, mas o caminho B é a decisão correta quando você não tem. Assim como no Caminho A, o Veeam Software Appliance executado como um appliance virtual ainda pode ser excluído na camada do hipervisor, portanto, implante em hardware físico sempre que possível.

O Caminho B pula a etapa inteira do Veeam Infrastructure Appliance. Se você escolher este caminho, avance da Etapa 2 (implantação do Veeam Software Appliance) diretamente para a Etapa 5 (tarefa de cópia de backup para o backup Vault).

Caminho C: Veeam Software Appliance + repositório NAS/Windows existente + Vault ou storage externo alternativo de terceiros: Este caminho aproveita a infraestrutura de storage existente e é menos protegido localmente, a menos que uma configuração adicional seja aplicada. Isso é útil quando os clientes querem utilizar parceiros existentes do Veeam Cloud & Service Provider (VCSP) para storage externo ou alternativas de storage externo que já tenham disponível.

Independentemente do seu caminho:

- Considere isolar o tráfego de backup em uma VLAN ou NIC dedicada para manter os dados de backup fora da sua rede de produção.
- Verifique sua cobertura de licenciamento de soquete/carga de trabalho antes da implantação.

Marco 2: Implante o Veeam Software Appliance e a infraestrutura

Implante o Veeam Software Appliance

- Faça o download do OVA do Veeam Software Appliance (para VMware vSphere) ou do ISO (para servidores físicos ou VMs em outros hipervisores compatíveis) no Portal do Cliente Veeam (my.veeam.com).
- Para OVA: Importe no VMware vSphere e ligue a máquina virtual. O Veeam Backup & Replication será acessível pela interface de gerenciamento após a primeira inicialização.
- Para ISO: Inicialize o servidor de destino (por exemplo, físico ou uma VM em qualquer outro hipervisor suportado) a partir da imagem ISO e siga o assistente de configuração. O Veeam Backup & Replication é instalado automaticamente.
- Conclua o assistente de configuração inicial do Veeam Software Appliance e defina o nome do host, as configurações de rede e as credenciais de administrador.

Conecte a infraestrutura ao Veeam Backup & Replication

- Adicione sua plataforma de virtualização ao inventário do Veeam Backup & Replication (Infraestrutura de Backup > Servidores Gerenciados).
- Adicione pelo menos um proxy de backup. Em ambientes menores, o Veeam Software Appliance pode servir como proxy inicial.
- Para ambientes VMware, configure o modo de transporte Hot-Add. A VM proxy monta os discos de origem usando SCSI e os acessa diretamente, evitando assim o caminho NBD mais lento pela rede de gerenciamento do ESXi.

Implantar o Veeam Infrastructure Appliance (caminho A)

- Faça o download do OVA ou ISO do Veeam Infrastructure Appliance no Portal do Cliente da Veeam.
- Implante usando o mesmo processo OVA/ISO do Veeam Software Appliance. Selecione repositório seguro ou proxy de backup como papel de destino durante o assistente de configuração.
- Depois de implantado, adicione o Veeam Infrastructure Appliance ao Veeam Backup & Replication como servidor gerenciado e, em seguida, configure-o como repositório de backup ou proxy de backup.
- Para a função de repositório seguro, adicione o repositório no Veeam Backup & Replication (infraestrutura de backup > repositórios de backup) e defina o período de retenção para imutabilidade.
- Ignore esta seção se estiver usando o Caminho B ou o Caminho C (já que nenhum Veeam Infrastructure Appliance é necessário).

O que o Veeam Software Appliance gerencia para você

O Veeam Backup & Replication está pré-instalado e pronto para configuração, sem a necessidade de configuração manual do sistema operacional, instalação de software ou aplicação de patches pré-implantação.

O Veeam Software Appliance é fornecido pré-protegido, com serviços desnecessários desativados, o sistema operacional bloqueado e as melhores práticas de segurança aplicadas por padrão.

Implante como um OVA no VMware vSphere, inicie a ISO em um servidor físico ou inicie dentro de uma VM em qualquer outro hipervisor suportado pela Veeam. Nenhuma experiência com Linux é necessária.

Instale o Veeam ONE

- O Veeam ONE possui um instalador separado para Windows. Atualmente, não é fornecido como parte do modelo de appliance.
- Instale o Veeam ONE em uma VM com Windows Server ou em um host físico (veja os requisitos mínimos no guia de implantação do Veeam ONE).
- Conecte o Veeam ONE ao Veeam Backup & Replication e ao seu host vCenter/Hyper-V durante o assistente de configuração.
- Configure as configurações de notificação de SMTP/e-mail imediatamente após a instalação. Você quer alertas ativos desde o primeiro dia.

Marco 3: Primeiros trabalhos de backup

- Crie seu primeiro job de backup para seu hipervisor primário. Direcione para o repositório seguro da Veeam (caminho A), o repositório local no Veeam Software Appliance (caminho B) ou o seu repositório NAS/Windows existente (caminho C).
- Configure uma política de retenção adequada para começar: 14 pontos de restauração diários, 4 semanais e 3 mensais (GFS).
- 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.

Primeiro teste de restauração — não pule!

Antes de passar para a fase 2, execute um Instant VM Recovery para uma VM 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.

O que o Veeam Infrastructure Appliance faz por você

Assim como o Veeam Software Appliance, o Veeam Infrastructure Appliance é entregue pré-reforçado e pré-configurado para a função designada. Nenhuma administração do Linux é necessária após a implantação.

Um único Veeam Infrastructure Appliance serve uma função: repositório seguro da Veeam ou proxy de backup. Se precisar de ambos, implante dois appliances.

Ele tem os mesmos formatos de implantação que o Veeam Software Appliance: OVA para VMware vSphere ou ISO para servidores físicos e outros hipervisores suportados.

FASE 2 • Dias 15 a 45

Otimizar

Objetivo: Proteção consistente, cópia em local externo e Visibilidade em todo o ambiente.

Marco 4: Processamento com percepção de aplicações

O processamento com percepção de aplicações garante que backups consistentes com desastres também se tornem consistentes com aplicações. Isso é crítico para cargas de trabalho transacionais, como SQL Server, Oracle, Exchange, Active Directory e outras cargas de trabalho aplicáveis.

- Habilite o processamento do sistema operacional convidado nos jobs de backup que abrangem servidores de aplicação Windows ou Linux.
- Configure o processamento com percepção de aplicações para SQL Server, Oracle, Exchange, controladores de domínio do Active Directory e outras cargas de trabalho aplicáveis.
- Defina uma política de truncamento de registros de transação quando aplicável e adequada às suas necessidades de recuperação.
- Após a primeira execução de um job com percepção de aplicações, confirme que os pontos de restauração estão marcados como consistentes com aplicações no Veeam Backup & Replication.
- Teste uma restauração no nível do item de Banco de dados SQL (ou de outras cargas de trabalho aplicáveis) usando o Veeam Explorer *for Microsoft SQL Server* para confirmar que a recuperação de aplicação de ponta a ponta funciona.

Marco 5:
Cópia de backup e Cofre

Este marco finaliza sua estratégia 3-2-1: uma cópia local no repositório primário e uma cópia imutável em um local externo. Esse é o alicerce arquitetônico do seu ambiente de backup.

Conectar Vault

- Adicione o Vault como um repositório de object storage no Veeam Backup & Replication (infraestrutura de backup > Object Storage Repositórios).
- Autentique-se com suas credenciais fornecidas pela Veeam e selecione sua região.
- Confirme que a imutabilidade está habilitada.

Jobs de cópia de backup

- Configure tarefas de cópia de backup com uma política de retenção GFS para manter pontos de restauração de longo prazo em local externo.
- Verifique se as tarefas de cópia fora do local foram concluídas com êxito e confirme se os objetos do Vault exibem os indicadores de imutabilidade no Veeam Backup & Replication.
- Realize uma restauração de teste do Vault para validar se a cópia fora do local está legível antes de considerar a Fase 2 como concluída.

Caminho C: opções de destino externo

Os caminhos A e B selecionam o Vault como destino para a cópia em local externo. O Caminho C pode usar o Vault ou um VCSP alternativo ou um repositório externo de terceiros, caso você já tenha um em operação. A imutabilidade é implementada por padrão em todos os Dados de backup armazenados no Vault. Se você direcionar para um local externo que não seja do Vault, confirme se a imutabilidade ou o bloqueio de objetos está configurado nesse repositório.

Marco 6: Monitoramento, Alertas e Configuração do Orchestrator

- Configure os destinatários de notificações de alarmes no Veeam ONE: alertas por e-mail para falhas em tarefas e Contratos de nível de serviço (SLAs) não cumpridos.
- Defina o horário operacional no Veeam ONE para alinhar os cálculos de SLA ao seu cronograma operacional.
- Revise os limites de alarmes padrão: desative ou ajuste alarmes irrelevantes ao seu ambiente para evitar a fadiga de alertas.
- Execute seus primeiros relatórios do Veeam ONE: relatório de VMs protegidas e relatório de sessões de tarefas.
- Analise o relatório de VMs desprotegidas e solucione quaisquer lacunas identificadas antes de prosseguir para a Fase 3.

Instale o Veeam Recovery Orchestrator (apenas na edição Premium)

Pule esta seção se sua edição for Foundation ou Advanced. O Veeam Recovery Orchestrator está incluído apenas na Veeam Data Platform Premium.

- O Veeam Recovery Orchestrator é um instalador separado para Windows. Ele pode residir juntamente com o Veeam ONE no mesmo host Windows ou ser executado em seu próprio host.
- Instale o Veeam Recovery Orchestrator em uma VM Windows Server ou em um host físico. Consulte os requisitos mínimos no guia de implantação do Veeam Recovery Orchestrator.
- Durante o assistente de configuração, conecte o Veeam Recovery Orchestrator à sua instância do Veeam Backup & Replication para que ele possa fazer o inventário das suas cadeias de backup existentes.
- Conecte o Veeam Recovery Orchestrator ao seu vSphere, Hyper-V ou Microsoft Azure para que a execução planejada possa ligar as VMs e atribuir redes corretamente.
- Opcionalmente conecte o Veeam Recovery Orchestrator ao Veeam ONE para obter dados de monitoramento mais completos e verificação baseada no DataLab.
- Aplique sua licença da Veeam Data Platform Premium para ativar o Veeam Recovery Orchestrator.
- Configure SMTP/email para que as notificações de execução planejada funcionem desde o primeiro dia.

FASE 3 • Dias 46—75

Resiliência de dados e resiliência dos negócios

Objetivo: Fechar as lacunas de proteção, melhorar RTOs/RPOs e adicionar resiliência a ransomware.

Marco 7: Fechar as Lacunas de Cobertura

- Execute o relatório de VMs desprotegidas no Veeam ONE para abordar todas as cargas de trabalho desprotegidas antes de qualquer outro ajuste.
- Estenda a proteção para cargas de trabalho físicas usando o Veeam Agent *for Microsoft Windows* ou o Veeam Agent *for Linux*, conforme necessário.
- Revise os agendamentos de tarefas em busca de conflitos e escalone os horários de início para evitar a contenção de recursos de proxy e repositório.
- Valide a conformidade com o RPO: Todas as VMs críticas estão gerando pontos de restauração dentro da sua janela de recuperação de destino?
- Confirme se todas as tarefas estão sendo concluídas dentro da sua janela de backup definida.

Adicionando capacidade de proxy com um segundo VIA

Se os jobs de backup estiverem lentos ou excederem a janela de backup, implante um segundo Veeam Infrastructure Appliance na função de proxy.

O modelo de appliance pré-protegido torna isso rápido: implante o OVA ou ISO, registre-o no Veeam Backup & Replication, e os jobs farão automaticamente o balanceamento de carga entre ambos os proxies, sem necessidade de configuração manual de proxy.

Marco 8: Prontidão contra Ransomware

- As edições Advanced e Premium do Veeam Data Platform incluem duas ferramentas de segurança complementares. O primeiro é o Recon, o serviço de inteligência de ameaças da Veeam que destaca IOCs e dados emergentes obtidos de respostas a incidentes reais. A segunda é o scan de backup, uma ação no produto Veeam Backup & Replication. Ele examina as cadeias de backup existentes em busca de indicadores de malware e valida a integridade dos arquivos, sem exigir uma rede isolada ou a inicialização de VMs.

Executar um backup de varredura:

- Crie um job SureBackup no Veeam Backup & Replication em Home > SureBackup. O SureBackup é executado como um trabalho agendado e pode analisar seus backups em busca de malware, ameaças com base em assinaturas e integridade de arquivos em um único fluxo, sem exigir uma rede isolada ou inicialização de VM para a própria verificação.

- Associe os jobs de backup que você deseja que sejam abrangidos, para que, ao longo do tempo, o job do SureBackup cubra todos os seus dados: Repositório Seguro da Veeam (Caminho A), repositório local do Veeam Software Appliance (Caminho B), o repositório NAS/Windows existente (Caminho C) e Vault.
- Nas opções de verificação, ative a análise de malware com o Veeam Threat Hunter (ou uma solução antivírus de terceiros) para comparar o conteúdo do backup com um banco de dados atual de assinaturas de ameaças.
- Nas mesmas opções de verificação, habilite a verificação de integridade de arquivo para validar o arquivo de backup com uma verificação CRC e identificar blocos corrompidos.
- Agende o job do SureBackup® e revise os resultados da sessão regularmente; investigue quaisquer pontos de restauração sinalizados antes de utilizá-los para recuperação.
- Para uma verificação ad hoc entre execuções agendadas, vá para Home > backups, expanda o job de backup, selecione a carga de trabalho e escolha Verificar backup na aba Backup.

Instale Recon

- Instale o binário Recon em qualquer host de infraestrutura Veeam com Windows ou em qualquer host Linux à sua escolha.
- O Recon também pode ser instalado em controladores de domínio do Windows aplicáveis.
- O Recon não pode ser instalado no Veeam Infrastructure Appliance. Os Veeam Infrastructure Appliances são de função única e pré-protegidos.

Auditoria de Imutabilidade

- Confirme se o período de imutabilidade no repositório seguro do seu Veeam Infrastructure Appliance está definido para uma janela de retenção apropriada.
- Verifique as configurações de criptografia de backup e habilite a criptografia em repouso nos jobs, se ainda não estiverem configuradas.
- Execute o relatório "Cargas de trabalho imutáveis" do Veeam ONE para medir e identificar alvos de imutabilidade de backup de cargas de trabalho.

Prontidão para recuperação de ransomware

Documente um plano de recuperação simples que inclua quais VMs restaurar primeiro, de quais pontos de restauração e para qual destino.

Identifique pelo menos um ponto de restauração limpo,anterior à infecção, no Vault como seu último ponto seguro conhecido.

Suas cópias imutáveis não podem ser sobrescritas ou criptografadas durante o período de imutabilidade. Esta é a sua rede de segurança.

Caminho A: Repositório seguro da Veeam e Vault.

Caminho B: storage local do Veeam Software Appliance e Veeam Vault.

Caminho C: Vault mais o seu repositório local, caso você tenha configurado a imutabilidade no repositório local.

Marco 9: Otimização de desempenho e planos de orquestração

- Analise a taxa de transferência de proxy nas estatísticas das tarefas do Veeam Backup & Replication. Se os jobs estiverem com gargalo, implante um segundo Veeam Infrastructure Appliance na função de proxy.
- Confirme se os Modos de transporte do backup estão otimizados: hot add (VMware) ou acesso direto ao storage, quando disponível.
- Confirme que todos os jobs de backup estejam concluídos dentro da sua janela de manutenção definida.
- Revise os gráficos de desempenho do Veeam ONE e identifique VMs com taxas de alteração excepcionalmente altas que possam se beneficiar de jobs dedicados ou cronogramas ajustados.

Crie os planos de orquestração iniciais (apenas para Premium)

Pule esta seção se a sua edição for Foundation ou Advanced ou se você não estiver usando um hipervisor suportado para o Veeam Recovery Orchestrator.

O Veeam Recovery Orchestrator transforma seu runbook de recuperação em um plano executável. Ao criar planos agora, a fase 4 pode demonstrar a recuperabilidade automaticamente, em vez de reexecutar restaurações manuais.

- Identifique as pilhas de aplicação Tier 1 que precisam de recuperação orquestrada (p. ex., controladores de domínio, banco de dados primário, servidores de aplicação primários).
- No Veeam Recovery Orchestrator, crie seu primeiro plano de restauração para uma dessas pilhas.
- Defina a ordem de inicialização das VMs e suas dependências para que os pré-requisitos (por exemplo, DCs, DNS, etc.) sejam iniciados antes dos serviços dependentes.
- Configure os destinos de recuperação (p. ex., host, cluster, datastore) e mapeie a rede de produção para failover de produção, além de uma rede isolada para testes.
- Defina os objetivos de RTO e RPO do plano para que o Veeam Recovery Orchestrator possa sinalizar desvios ao longo do tempo.
- Salve o plano e revise a documentação gerada automaticamente com as partes interessadas antes de declarar a Fase 3 concluída.

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.

SureBackup e verificação de backup

- Configure um Grupo de Aplicação SureBackup® que cubra suas VMs mais críticas (p. ex., controladores de domínio, servidores de aplicação principais).
- Execute um job SureBackup® para automatizar a verificação de inicialização e confirmar que as VMs iniciam e passam nos testes de heartbeat, ping e no nível da aplicação.
- Para uma verificação mais leve, execute um Scan Backup. Valida a integridade dos arquivos e verifica se há ameaças sem inicializar as VMs, sendo um complemento prático ou uma alternativa ao SureBackup em ambientes menores.

Testes de restauração granular e completa

- Realize testes de restauração no nível do arquivo e recupere arquivos individuais de um backup para um local de teste.
- Teste a recuperação de itens de aplicação restaurando um objeto de banco de dados SQL ou um usuário do Active Directory usando Veeam Explorers.
- Teste uma restauração de VM completa a partir do Vault para simular uma perda total no local e validar sua cópia no local externo.
- Registre os tempos de recuperação reais, compare-os com suas metas de RTO e 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.

Executar planos de orquestração (apenas para Premium)

Pule esta seção se a sua edição for Foundation ou Advanced, ou se o seu hipervisor não for suportado pelo Veeam Recovery Orchestrator. A fase 3 criou seu primeiro plano de restauração, mas a fase 4 é onde ele mostra seu valor.

- Execute um teste de prontidão autônomo em seu plano. O Veeam Recovery Orchestrator verifica a disponibilidade do ponto de restauração, a capacidade de destino e o desvio de configuração, sem precisar inicializar nenhuma VM.
- Realize um teste DataLab no seu plano. O Veeam Recovery Orchestrator restaura a pilha de aplicações em uma rede isolada e executa verificações de nível de aplicação em VMs ativas.
- Registre os tempos de recuperação reais da execução do DataLab e compare-os com a meta de RTO definida na Fase 3.
- Gere o relatório de prontidão de recuperação do Veeam Recovery Orchestrator e arquive-o junto com os resultados dos seus outros testes de recuperação.
- Para cargas de trabalho não cobertas por um plano do Veeam Recovery Orchestrator, recorra aos testes de restauração manual acima.

Marco 11: Relatórios e Documentação

Gere um relatório mensal de sumário executivo do Veeam ONE e envie à administração para demonstrar a integridade do backup e a cobertura do backup.

- Exporte um relatório de inventário de cargas de trabalho protegidas para confirmar o escopo da cobertura.
- Documente sua arquitetura final de backup, incluindo lista de jobs, layout do repositório, funções do Veeam Infrastructure Appliance, cronogramas 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.
- Exclusivo para clientes Premium: gere o relatório de prontidão de recuperação do Veeam Recovery Orchestrator mensalmente. Acompanhe a pontuação de prontidão ao longo do tempo, conforme as cargas de trabalho e dependências mudam.
- Exclusivo para clientes Premium: Arquive a documentação do plano gerada pelo Veeam Recovery Orchestrator junto à documentação de arquitetura. O Veeam Recovery Orchestrator regenera automaticamente isso quando os planos mudam, então arquive novamente quando os planos forem atualizados.

Marco 12:
Cadência de higiene contínua

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

- **Semanalmente:** Analise o painel de integridade das tarefas do Veeam ONE etrate imediatamente falhas ou avisos.
- **Semanalmente:** Analise o relatório de VMs desprotegidas no Veeam ONE e implemente proteção para novas VMs.
- **Mensalmente:** Gere um sumário executivo e relatórios de VMs protegidas e compartilhe os resultados.
- **Mensalmente:** Revise o consumo de storage do Vault e a taxa de crescimento. Avise se estiver excedendo o espaço ocupado previsto no orçamento ou se houver próximos aumentos de retenção.
- **Mensalmente:** Confirme que as janelas de retenção ainda estão ativas e não modificadas.
- **Trimestralmente:** Faça um teste de recuperação documentado e varie os tipos de carga de trabalho.
- **Trimestralmente:** Execute uma varredura de backup em cada repositório para verificar assinaturas de malware e alterações na integridade dos arquivos.
- **Trimestralmente:** Revise quem tem acesso administrativo ao Veeam Backup & Replication, Veeam ONE e Veeam Recovery Orchestrator (somente Premium). Remova o acesso para qualquer pessoa que tenha mudado de função ou saído.
- **Trimestralmente (apenas Premium):** Realize um teste do DataLab do Veeam Recovery Orchestrator e alterne qual plano de orquestração é testado.
- **Trimestralmente (apenas para a edição Premium):** Gere novamente e arquive a documentação dos planos do Veeam Recovery Orchestrator caso algum plano tenha sido alterado desde a última revisão.
- **Mensalmente:** Revise as atualizações de inteligência de ameaças do Recon e aplique assinaturas ou regras relevantes ao seu ambiente.

- **Anualmente:** Revise sua arquitetura de backup e políticas de retenção em relação aos requisitos atuais dos negócios e quaisquer novas obrigações de conformidade.

- **Anualmente:** Faça uma restauração completa a partir do Vault para validar se a cópia externa é recuperável de ponta a ponta. Documente o resultado.

- **Anualmente:** Revise as configurações de criptografia em transmissão e em repouso e faça a rotação das chaves de acordo com sua política de segurança.

- **Conforme necessário:** Planeje a cadência de atualização dos seus componentes Veeam (por exemplo, Veeam Software Appliance, Veeam Infrastructure Appliance, Veeam ONE, Veeam Agents e Veeam Recovery Orchestrator, se aplicável) e inscreva-se para receber notificações de atualizações.

- **Antes da renovação:** Reveja o uso do licenciamento, as projeções de crescimento e a compatibilidade da edição. Se você já ultrapassou o conjunto de recursos da sua edição, este é o momento de discutir um upgrade com seu representante da Veeam.

Recomendações Finais

Parabéns! Você conseguiu!

Em 100 dias, você passou da implantação para um ambiente de proteção de dados totalmente operacionalizado. Suas cargas de trabalho estão protegidas, seus backups estão reforçados e imutáveis, e você comprovou que pode recuperar não só na teoria, mas com registro.

Isso não é pouca coisa.

Agora, o foco muda da construção para a manutenção. Mantenha as restaurações em um cronograma regular de testes, ajuste as políticas conforme o ambiente evolui e utilize sua cadência de monitoramento e geração de relatórios para identificar desvios antes que se tornem riscos. Os hábitos que você estabeleceu no Marco 12 — sua rotina de higiene semanal, mensal, trimestral e anual — são o que garantem a integridade do seu ambiente muito além do Dia 100. Siga-os, adote-os e evolua-os à medida que sua organização cresce.

Lembre-se, o Dia 100 não é a linha de chegada. É a referência inicial. A resiliência é uma prática, não um projeto.

Mantenha suas funções de administrador atualizadas para que as pessoas certas tenham sempre o acesso correto, e permaneça inscrito nas notas de lançamento e avisos de segurança da Veeam para nunca ser pego de surpresa.

Você Não Precisa Fazer Isso Sozinho

As comunidades, os recursos de aprendizagem e as equipes técnicas da Veeam existem para ajudar você a ir além. Utilize esses recursos à medida que seu ambiente cresce e amadurece! Uma lista selecionada de recursos está disponível no apêndice.

Em caso de dúvidas ou próximas etapas, entre em contato com o seu Gerente de Sucesso do Cliente ou com Suporte Técnico da Veeam para questões técnicas.

Apêndice: Referência rápida

Componentes Principais: Veeam Data Platform

- **Veeam Software Appliance:** Um appliance pré-endurecido com o Veeam Backup & Replication pré-instalado. Implante em formato OVA (VM) ou ISO (físico). Este é o ponto de partida recomendado para todas as implantações de PMEs.
- **Veeam Infrastructure Appliance:** Um appliance pré-hardenizado implantado como um proxy de backup dedicado ou repositório seguro. Ele fornece imutabilidade local sem necessidade de conhecimento em Linux, com uma função por appliance.
- **Veeam Backup & Replication:** Uma solução central de backup, hospedada no Veeam Software Appliance. Gerencia tarefas, repositórios, proxies e operações de recuperação.
- **Veeam ONE:** Realiza monitoramento, alertas e relatórios. Possui uma instalação separada baseada em Windows e conecta-se ao Veeam Backup & Replication e ao seu hipervisor para visibilidade completa da pilha.
- **Recon:** Esse é o serviço de inteligência de ameaças da Veeam. Apresenta indicadores de comprometimento (IoCs), assinaturas de ameaças e dados de campanhas emergentes extraídos de respostas a incidentes reais. Incluído no Veeam Data Platform Advanced.
- **Verificar o conteúdo do backup:** Esta é uma ação do produto que verifica cadeias de backup existentes em busca de assinaturas de malware conhecidas e valida a integridade dos arquivos, sem exigir uma rede isolada ou inicialização de VMs. Incluído no Veeam Data Platform Advanced.
- **Veeam Recovery Orchestrator:** Uma plataforma de orquestração que automatiza a recuperação de desastres (DR) no nível da aplicação. Permite criar planos de restauração executáveis, executar testes de prontidão, realizar verificações com o DataLab e gerar documentação de recuperação. Incluído na Veeam Data Platform Premium Edition.
- **Veeam Data Cloud Vault:** Fornece storage de objetos em nuvem imutável para cópias em local externo. É gerenciado pela Veeam, sem necessidade de uma conta de nuvem separada.

Termos-chave

- **Objetivo de ponto de recuperação (RPO):** Perda de dados máxima aceitável, medida em tempo. Determina a frequência do agendamento de backups.
- **Recovery time objective (RTO):** Tempo máximo de inatividade aceitável antes que uma carga de trabalho precise ser recuperada.
- **Grandfather-Father-Son (GFS):** Esquema de retenção que mantém pontos de restauração diários, semanais e mensais.
- **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.
- **Instant VM Recovery:** Restaura uma VM diretamente de um backup em segundos, sem a necessidade de copiar os dados previamente. Sempre migre para o armazenamento de produção após a validação.
- **Plano de orquestração (Veeam Recovery Orchestrator):** Um runbook executável que define a ordem, dependências, locais de destino e mapeamentos de rede para restaurar um conjunto de cargas de trabalho. Substitui um runbook manual de recuperação por uma automação autodocumentada e testável.
- **DataLabs:** Ambiente de teste isolado no qual o Veeam Recovery Orchestrator (ou SureBackup) restaura um backup e executa a verificação no nível da aplicação sem afetar a produção. Permite testes completos de planos em qualquer frequência.
- **Processamento com percepção de aplicações:** Processamento do sistema convidado que cria pontos de Backup consistente com aplicação para SQL Server, Oracle, Exchange, Active Directory, SharePoint, PostgreSQL e MySQL. Utiliza VSS no Windows e scripts de pré-congelamento e pós-congelamento, além de quiescência nativa do banco de dados no Linux.
- **Veeam Hardened Repository:** Um repositório de backup baseado em Linux com imutabilidade imposta no nível do sistema de arquivos. O Veeam Infrastructure Appliance oferece um repositório seguro da Veeam pré-configurado, sem necessidade de administração Linux. Object storage e bloqueio de objetos são mecanismos de imutabilidade distintos, não equivalem aos repositórios Hardened da Veeam. A imutabilidade no nível do sistema de arquivos protege contra ataques no SO, mas não contra a destruição no nível da VM. Um repositório seguro da Veeam executado como um appliance virtual ainda pode ser excluído na camada do hipervisor; portanto, implemente o Appliance de infraestrutura da Veeam em hardware físico para garantir a máxima proteção.
- **Hot-Add transport mode:** Este é um método de transporte de backup específico do VMware. A VM proxy realiza o hot add dos discos virtuais da VM de origem e os lê via SCSI, evitando o caminho NBD na rede de gerenciamento ESXi.

Apêndice: Links Úteis

Minha conta

Sua conta Veeam é seu hub central para gerenciar sua implantação. Uma vez conectado, você pode fazer o download de produtos e chaves de licença, gerenciar administradores de caso, entrar em contato com o Suporte Veeam e renovar contratos ou adicionar licenças.

- Faça login ou crie sua conta Veeam
- Como criar uma conta
- Perguntas frequentes sobre login
- Gerenciamento de funções de administrador de licenças e/ou casos

Documentação e downloads

- Central de Ajuda com documentação técnica, diretrizes de implantação e guias do usuário
- Downloads de produtos incluindo atualizações de software, patches e Notas de lançamento
- Base de Conhecimento de Suporte com problemzas comuns, etapas de solução de problemas e resoluções recomendadas, atualizada regularmente pelas equipes de Suporte Veeam e Engenharia da Veeam

Aprendizado e Melhores Práticas

- Webinars de integração ao vivo: Webinars de integração ao vivo regulares, nos quais você pode fazer perguntas em tempo real e ouvir diretamente de especialistas técnicos
- Veeam University FREE: cursos em seu próprio ritmo e certificações sem custo
- Calculadoras de Dimensionamento Veeam: ferramenta online de dimensionamento e estimativa usada para calcular os requisitos de infraestrutura, storage e capacidade para implantações do Veeam
- Melhores práticas dos Arquitetos de Soluções Veeam: Diretrizes de design e configuração de infraestrutura baseadas em implantações reais, recomendadas para revisão à medida que seu ambiente evolui.
- Sugestões práticas para a Veeam Intelligence: Uma coleção selecionada de sugestões eficazes para ajudar você a explorar todo o potencial da Veeam Intelligence
- Veeam Search: portal de pesquisa centralizado da Veeam para pesquisar recursos da Veeam em um só lugar

Comunidades da Veeam

- Fóruns da comunidade Veeam: Conecte-se com colegas, compartilhe melhores práticas, participe de Grupos de Usuários e eventos da comunidade, e fale sobre casos de uso reais
- Fóruns de P&D da Veeam: Sua linha direta com a equipe de P&D da Veeam para conversas sobre produtos, dúvidas técnicas e feedback sobrerecursos

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 X @veeam.