ELIZEU MOREIRA DA SILVA

ESTUDO DE CASO SOBRE A IMPLEMENTAÇÃO DE UMA INFRAESTRUTURA DE BACKUP NA EMPRESA X

Ji-Paraná
2023

ELIZEU MOREIRA DA SILVA

ESTUDO DE CASO SOBRE A IMPLEMENTAÇÃO DE UMA INFRAESTRUTURA DE BACKUP NA EMPRESA X

Monografia apresentado à Banca Examinadora do Curso de Sistemas de Informações do Centro Universitário São Lucas Ji-Paraná, como requisito de aprovação para obtenção do Título de Bacharel em Sistemas de Informação.

Orientador: Prof. Esp. Romário Vitorino Ferreira

Ji-Paraná
2023

Dados Internacionais de Catalogação na Publicação - CIP

S586e Silva, Elizeu Moreira da.

Estudo de caso sobre a implementação de uma infraestrutura de backup na empresa X. / Elizeu Moreira da Silva. – Ji-Paraná, 2023.
47 p.; il.

Trabalho de Conclusão de Curso (Sistemas de Informação) – Centro Universitário São Lucas Ji-Paraná, 2023.

Orientador: Prof. Esp. Romário Vitorino Ferreira.

1. Backup. 2. Veeam Backup. 3. VMware. 4. Google Cloud. I. Ferreira, Romário Vitorino. II. Título.

CDU 004.658

Ficha Catalográfica Elaborada pelo Bibliotecário Giordani Nunes da Silva CRB 11/1125

ELIZEU MOREIRA DA SILVA

ESTUDO DE CASO SOBRE A IMPLEMENTAÇÃO DE UMA INFRAESTRUTURA DE BACKUP NA EMPRESA X

Trabalho de Conclusão de Curso apresentado à Banca Examinadora do Centro Universitário São Lucas Ji-Paraná, como requisito de aprovação para obtenção do Título de Bacharel em Sistemas de Informação.

Orientador: Prof. Esp. Romário Vitorino Ferreira

Ji-Paraná, 19 de junho de 2023

Avaliação/Nota:

BANCA EXAMINADORA

_____
Prof. Esp. Romário Vitorino
Orientador
Centro Universitário São Lucas Ji-Paraná

_____
Prof. Ma. Ana Flávia M. Camargo
Examinadora
Centro Universitário São Lucas Ji-Paraná

_____
Prof. Esp. Alisson Stork Coelho
Examinador
Centro Universitário São Lucas Ji-Paraná

AGRADECIMENTOS

A você, que dispôs de um pouco do seu tempo para prestigiar este trabalho.

RESUMO

O backup de dados é uma prática imprescindível para garantir a disponibilidade e a integridade de informações, protegendo-as contra perdas acidentais ou intencionais. Este trabalho, tem como intuito apresentar um estudo de caso sobre a implementação de uma infraestrutura de backup em uma empresa X localizada no município de Ji-Paraná, no estado de Rondônia. Apresentando os conceitos base de backup, os tipos mais comuns, melhores práticas para a utilização, e a implementação de uma infraestrutura de backup utilizando a ferramenta Veeam Backup and Replication, a partir de um servidor VMware, com envio para um storage local e para a nuvem pública Google Cloud, assim como as etapas necessárias para sua execução. Ademais, serão abordadas questões relacionadas à segurança, recuperação de desastres e testes de recuperação. Com base nos resultados positivos das métricas de backup empregadas, espera-se que este trabalho seja útil para outras empresas da região possam implementar uma infraestrutura de backup confiável e eficiente.

Palavras-chaves: Backup. Veeam Backup. VMware. Google Cloud

ABSTRACT

Data backup is an essential practice to ensure the availability and integrity of information, protecting it against accidental or intentional loss. This work aims to present a case study on the implementation of a backup infrastructure in a company X located in the municipality of Ji-Paraná, in the state of Rondônia. Introducing the basic concepts of backup, the most common types, best practices for use, and the implementation of a backup infrastructure using the Veeam Backup and Replication tool, from a server textitVMware, with sending to a local storage and to the public cloud Google Cloud, as well as the necessary steps for its execution. In addition, issues related to security, disaster recovery and recovery tests will be addressed. Based on the positive results of the employed backup metrics, it is expected that this work will be useful for other companies in the region to implement a reliable and efficient backup infrastructure.

Keywords: Backup. Veeam Backup. VMware. Google Cloud

LISTA DE FIGURAS

LISTA DE ABREVIATURAS E SIGLAS

VM	Virtual Machine
GDPI	Global Data Protection Index
GDPR	Regulamento Geral de Proteção de Dados
LGPD	Lei Geral de Proteção de Dados
RPO	Recovery Point Objective
RTO	Recovery Time Objective
TI	Tecnologia da Informação
AD	Active Directory

SUMÁRIO

1. INTRODUÇÃO

Com o avanço tecnológico e a exponencial dependência dos sistemas de informação, os dados tornam-se um ativo valioso para empresas, organizações e a sociedade de modo geral. Em face disso, (POSTHUMUS S.; VON SOLMS, 2004) faz alusão às falhas de segurança, invasões ou a corrupção de arquivos comprometem as informações e ocasiona em exemplos de desastres na que causar prejuízos financeiros perante corporações. Nesse contexto, a implementação de uma política de *backup* é crucial para a proteção de dados e a disponibilidade e de informações.

No campo da informática, o termo *backup* deriva do vocabulário inglês e possui sua etimologia traduzida como "ajuda" ou "apoio". De acordo com o (DICIO, 2023) está diretamente relacionado às cópias de segurança que se faz regularmente para assegurar que um arquivo ou o conjunto de dados de um computador, ou celular, não se perca, sendo usado quando há prejuízo ou dano no arquivo original.

(GOMES, 2015) salienta a relevância da implantação de um eficiente sistema de *backups* em uma organização, sendo uma estratégia imprescindível e abrangente no gerenciamento de informações. Neste estudo é apresentada uma solução que visa mitigar o impacto destes incidentes, descrevendo o estabelecimento de uma infraestrutura de *backup* eficiente e confiável utilizando a ferramenta *Veeam Backup and Replication* que executará o processo de *backup* a partir de uma infraestrutura *VMware*[1] *c*ontendo duas máquinas virtuais *(VMs)*.

Para implantação desta solução, diversos artigos, sites e livros foram consultados a respeito da segurança da informação. Assim, o objetivo geral deste estudo é apresentar uma infraestrutura de *backup* abordando a análise de diferentes metodologias de backup, armazenamento e recuperação de dados de máquinas virtuais. Além disso, possui integração com *Google Cloud*[2] permitindo o uso de serviços adicionais, como cópia de *backups* entre diferentes regiões geográficas, o que aumenta ainda mais a disponibilidade de dados.

Esse cenário justifica o presente trabalho, que visa orientar a

[1] A VMware produz software e serviços para computação em nuvem e virtualização, o que permite criar máquinas virtuais. Para mais informações: https://www.vmware.com/br.html

[2] Disponível em: https://cloud.google.com/?hl=pt-br. Acesso em: 15 de junho de 2023

implementação dos processos para realização de backup utilizando o *Veeam Backup and Replication* com destino na nuvem pública *Google Cloud*, de forma a guiar outras empresas que buscam uma solução de proteção de dados abrangente, confiável e escalável para sua organização.

Dessa forma, espera-se que esta pesquisa contribua para o meio a que se insere, através de uma visão ampla sobre o assunto, acrescendo com resultados obtidos na consideração da implementação de infraestruturas de backup.

1.1. OBJETIVO GERAL

O objetivo geral deste trabalho é apresentar a implementação de uma rotina de backup utilizando o software *Veeam Backup and Replication*[3] associado a três máquinas virtuais (VMs), com cópia para *storage*[4] local e o serviço de nuvem pública *Google Cloud*. Vamos explorar os objetivos específicos de implementação dessa infraestrutura em uma empresa X:

1.2. OBJETIVOS ESPECÍFICOS

- Realizar o levantamento de requisitos de uma infraestrutura *backup*;
- Realizar testes de recuperação para verificar a eficácia do processo de *backup*;
- Avaliar o desempenho da infraestrutura de *backup*, considerando o tempo de *backup* e eficiência no uso de espaço de armazenamento;
- Analisar a segurança e confiabilidade da solução implementada;
- Apresentar recomendações e considerações finais sobre a utilização do *Veeam Backup and Replication* para *backup* de infraestruturas *VMware*.

[3] Disponível em: https://www.veeam.com/vm-backup-recovery-replication-software.html?ad=menu-products. Acesso em: 15 de Junho de 2023

[4] O vocábulo deriva do inglês e refere-se a unidades storage, ou seja, espaço para armazenagem

2. REFERENCIAL TEÓRICO

2.1. BACKUP: CONCEITO E IMPORTÂNCIA

Um *backup* é uma cópia dos dados originais armazenados em um sistema de computador, com o intuito de proteger e armazenar as informações em caso de desastres, corrupção e/ou eliminação acidental dos dados. Segundo a (GDSOLUTIONS, 2016), o principal objetivo de um *backup* é a cópia de dados para restauração em caso de perda, alteração não autorizada ou danos a algum tipo de arquivo ou sistema digital. Ele é essencial para garantir a disponibilidade contínua das informações críticas de uma organização ou indivíduo.

Sua notoriedade relaciona-se à necessidade de garantir a preservação de informações sensíveis ou não, a minimização dos riscos de perda de dados e a continuidade dos negócios. A perda de dados pode ser ocasionada por diversos fatores, como falhas de *hardware*, erros humanos, ataques cibernéticos, desastres naturais ou incêndios.

O estudo *Global Data Protection Index* (GDPI)[5] realizado no ano de 2022 pela *Dell Tecnologies* demonstra que:

- 67% dos entrevistados estão preocupados em lidar com *malware* e *ransomware*;
- 70% consideram o risco de ameaças cibernéticas maior com funcionários remotos;
- 67% não estão confiantes que dados em nuvens públicas estão seguros.

A temática traz como reflexo os desafios do modelo *home office* durante a pandemia, a preocupação com a segurança digital, explosão no número de dados corporativos, soluções atuais para proteção de dados e ataque cibernético.

2.2. TIPOS DE BACKUP

Dentre os vários tipos de *backup*, cada um desempenha sua função de acordo com suas finalidades específicas. Abaixo estão descritos os tipos de

[5] Disponível em: https://www.dell.com/pt-br/dt/data-protection/gdpi/index.htmscroll=off Acesso em 8 de junho. 2023

backup, consoante com (NETO et al., 2014):

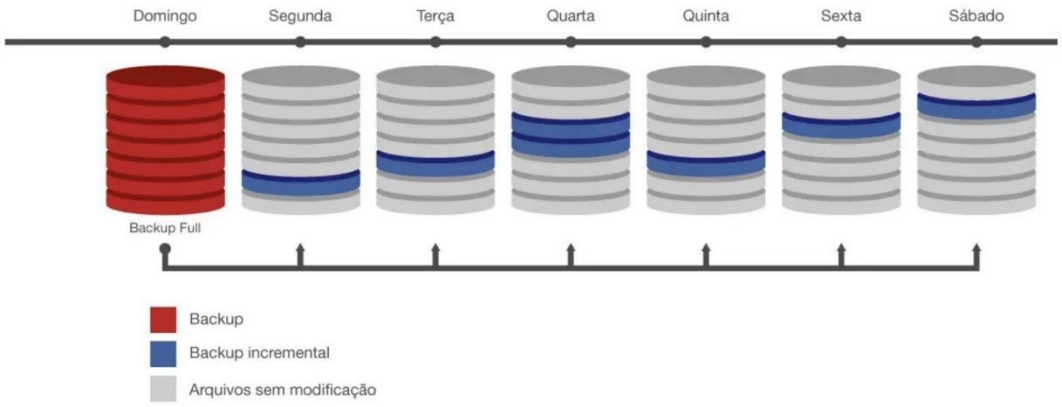
1. *Backup* Completo: abrange a cópia de todos os dados e arquivos em um sistema. É útil para a recuperação completa dos dados, mas pode ser demorado e exigir mais espaço de armazenamento, como mostra a Figura 1.

Figura 1 – Backup Completo

Fonte: (CONTROLE. . . ,)

2. *Backup* Incremental: consiste em copiar apenas os arquivos que foram alterados desde o último *backup*. Isso reduz o tempo e o espaço necessários para o *backup*, mas sua recuperação pode ser mais demorada, pois é necessário restaurar o *backup* completo e aplicar os *backups* incrementais subsequentes, como na Figura 2.

Figura 2 – Backup Incremental

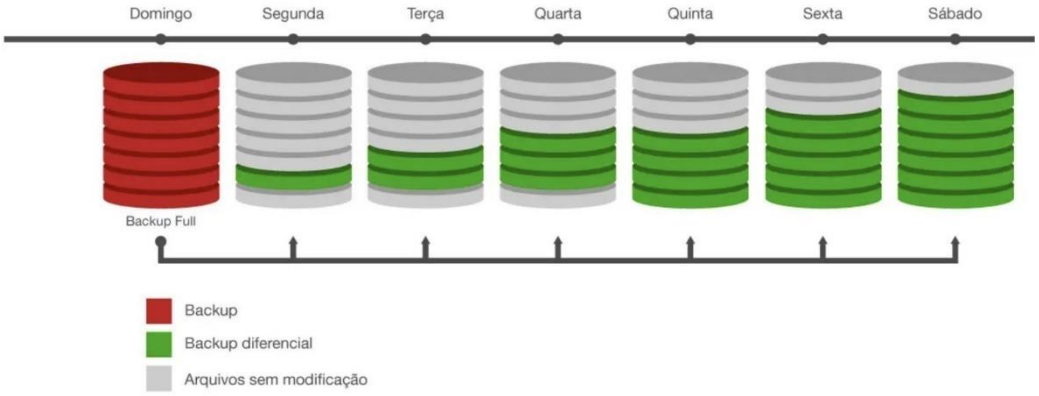


Fonte: (CONTROLE. . . ,)

3. *Backup* Diferencial: compreende a cópia apenas dos arquivos que foram modificados desde o último *backup* completo. É mais rápido do que o *backup* incremental durante a restauração, pois requer apenas o último *backup*

completo e o *backup* diferencial mais recente, como indica a Figura 3.

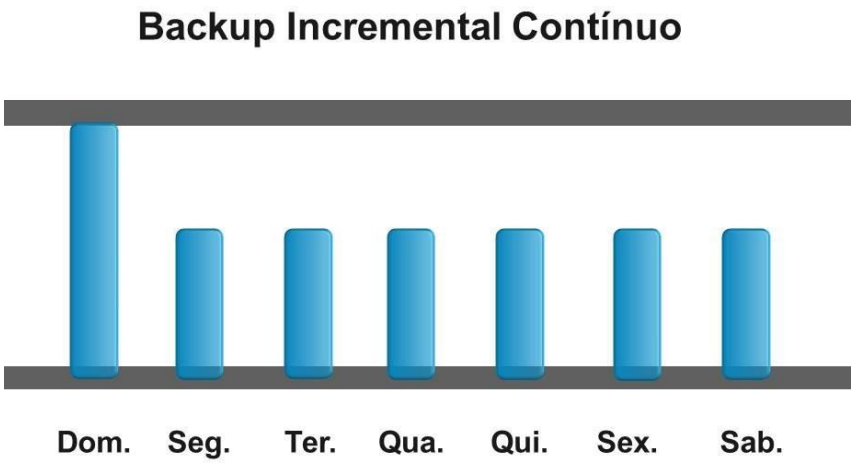
Figura 3 – Backup Diferencial



Fonte: (CONTROLE. . . ,)

4. *Backup* Contínuo: realiza cópias dos dados em tempo real ou em intervalos curtos e frequentes. É ideal para sistemas que exigem uma recuperação rápida e que não podem perder muitos dados, que pode ser demonstrado na Figura 4.

Figura 4 – Backup Contínuo



Fonte: (SPANIOL,)

2.3. MELHORES PRÁTICAS

Ao implementar uma infraestrutura de *backup*, é importante que sejam estabelecidas as melhores métricas para que haja eficácia e a segurança dos

dados, através de um criterioso planejamento. A seguir, serão detalhados alguns desses parâmetros (NAIK,):

1. Definir uma política de *backup*: neste passo, são definidos quais os dados e sistemas precisam ser copiados, com qual frequência e por quanto tempo eles devem ser mantidos. Esse é o processo que determina a importância dos dados e as necessidades de recuperação dos mesmos.
2. Indicar a estratégia de *backup* adequada: aqui é considerado o tipo de *backup* mais pertinente para cada conjunto de dados. É uma fusão de 3 (três) tipo de *backups*: o *backup* completo, incremental e diferencial que visam otimizar a eficiência e o tempo de recuperação dos dados.
3. Armazenar os *backups* em local adequado: manter as cópias de *backup* em um local seguro, protegido contra acesso não autorizado, falhas de *hardware* e até mesmo desastres naturais, é primordial. O armazenamento em nuvem é uma boa prática para garantir a disponibilidade e segurança dos *backups*.
4. Criptografar os backups: utilizar a criptografia para proteger os dados sensíveis durante o armazenamento e a transmissão dele. Isso permite que o acesso não autorizado aos dados seja evitado, garantindo sua confidencialidade.
5. Testar regularmente os *backups*: a realização de testes periódicos de recuperação para constatar a verificação e a integridade dos *backups*, junto com a eficácia dos procedimentos de recuperação, garante que os dados possam ser restaurados com sucesso em caso de necessidade.

2.4. SEGURANÇA DOS DADOS E CRIPTOGRAFIA

A segurança dos dados é uma preocupação vital ao lidar com *backups*. Além das práticas mencionadas acima, a criptografia desempenha um papel substancial na proteção dos dados durante o armazenamento e a transmissão dos mesmos. Existem regulamentações e leis de proteção de dados, como o Regulamento Geral de Proteção de Dados (GDPR)[6] na União Europeia e a Lei Geral de Proteção de Dados (LGPD)[7] no Brasil, que estabelecem diretrizes

[6] Disponível em: https://commission.europa.eu/law/law-topic/data-protection-pt. Acesso em: 05 de junho de 2023

[7] Disponível em: https://www.planalto.gov.br/ccivil03/ato2015-2018/2018/lei/l13709.htm. Acesso em: 05 de junho de 2023

específicas para a proteção dos dados pessoais, incluindo a necessidade de criptografia em determinados contextos.

De acordo com a (IBM, 2023), a criptografia envolve a conversão dos dados em um formato ilegível, conhecido como texto cifrado, usando algoritmos matemáticos. Somente aqueles que possuem a chave correta aplicada durante todo o processo de *backup*, desde sua captura, armazenamento e transmissão, fazendo com que mitigue riscos. Ademais, é importante gerenciar adequadamente as chaves de criptografia, garantindo sua segurança e disponibilidade.

2.5. Recuperação de Desastres e Testes de Recuperação

Um ambiente digital pode ser demasiadamente comprometido ou até mesmo tornar-se inoperante. (AL- OMARI R.; SOMANI, 2004), ressalta que um fator em relação à gestão dos backups é o agendamento, no qual possibilita a recuperação de recentes versões de dados. Nesse caso, é essencial ter um plano de recuperação de desastres bem definido, que inclua procedimentos para restauração dos *backups*.

Uma delas é a criação de um site de para obtenção de recuperação, que também é conhecido como site de contingência ou site secundário. Nesse modelo, há uma réplica dos sistemas e dados críticos é mantida em um local geograficamente distante do local principal, para que em casos emergenciais, os dados sejam recuperados a partir do site secundário, permitindo a retomada das operações de forma mais rápida e eficiente. Outra tática é a implementação de *backups* em diferentes camadas, como *backups* locais e *backups* na nuvem. Os *backups* locais são essenciais para uma recuperação rápida e eficiente em casos de falhas menores, enquanto os *backups* na nuvem oferecem uma camada adicional de segurança, permitindo que os dados sejam recuperados mesmo em situações de desastres que afetam o ambiente local.

Além disso, em casos de falhas é indispensável a realização de testes regulares de recuperação. Eles consistem em uma simulação na qual os dados são restaurados em um ambiente controlado para verificar se o processo é bem-

sucedido e se os dados recuperados estão corretos e operáveis ou não. São capazes de identificar eventuais falhas nos procedimentos de *backup*, como falha na integridade dos dados, incompatibilidades entre os sistemas ou erros na configuração. A periodicidade de realização dos testes fornece eficácia e confiabilidade no processo de recuperação de um *backup*.

3. MATERIAIS E MÉTODOS

3.1. LEVANTAMENTO DE REQUISITOS NA EMPRESA X

Este estudo classifica-se em caráter aplicado, pois tem o objetivo de gerar conhecimentos para aplicação prática, conduzidos à solução de problemas específicos (SILVA E. L., 2005). Nesta seção, iremos abordar as necessidades da empresa X em relação à infraestrutura de backup, considerando os seguintes aspectos baseados em (ROTARU, 2012) e (SENGUPTA SHUBHASHIS E ANNERVAZ, 2014):

- O volume de dados: onde é estimado o tamanho total dos dados que serão incluídos no processo de backup;
- RPO (Recovery Point Objective): sendo o intervalo de tempo aceitável entre os pontos de recuperação dos dados;
- RTO (Recovery Time Objective): o tempo máximo tolerável para a recuperação de dados;
- Retenção de dados: os requisitos de retenção de dados;
- Recursos de infraestrutura existentes: recursos de hardware adequados, como CPU, RAM e armazenamento.

3.2. DEFINIÇÃO DE REQUISITOS DO BACKUP

Neste tópico, identificamos os requisitos específicos do backup, sendo:

- A frequência do backup: a cada 12hs;
- A janela de backup: a cada 12hs;
- A retenção do backup: 2 dias;
- A recuperação de desastres (restore).

3.3. INFRAESTRUTURA DO BAKCUP

Nesta alínea, é descrita a infraestrutura de backup adequada aos requisitos relatados na seção 3.1 e seção 3.2. Sua execução é simulada em ambiente controlado, semelhante a um cenário real, formado por 2 servidores físicos, onde a infraestrutura do Veeam Backup and Replication possui arquitetura integrada a um esxi8 associado a um storage local, designado dentro do próprio servidor do Veeam Backup and Replication e outro para a nuvem pública Google Cloud.

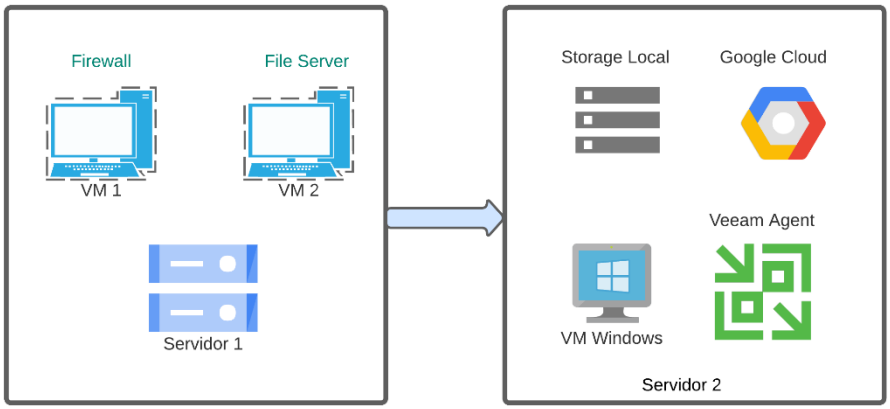
- Servidor 1: possui um ESXi[8] na versão 8.0 instalado, composto por 2 máquinas virtualizadas: a primeira denominada como *Firewall* e outra como *File Server* ;
- Servidor 2: contém o sistema operacional *Windows* (MICROSOFT, 2022) e o *Veeam Backup and Replication* (SOFTWARE, 2023) na versão 12, devidamente instalado e configurado.

Abaixo, temos a representação de sua arquitetura:

3.4. IMPLEMENTAÇÃO DO PLANO DE BACKUP

Nesta subseção, é apresentado o *software Veeam Backup and Replication* e sua configuração, o processo para armazenamento na nuvem pública *Google Cloud*, a configuração dos *jobs*[9] de *backup*, a cópia e restauração das VM.

Figura 5 – Arquitetura da infraestrutura



Fonte: Elaborado pelo autor

3.4.1. O Veeam Backup and Replication

O *Veeam Backup and Replication*[10] é um produto de *software* desenvolvido pela *Veeam Software* para fazer *backup*, restaurar e replicar dados

[8] ESXi é uma plataforma de virtualização na qual você pode criar e executar máquinas virtuais virtuais e dispositivos virtuais. Para mais informações: https://docs.vmware.com/br/VMware-vSphere/8.0/vsphere-esxi-80-upgrade-guide.pdf

[9] Termo comumente utilizado para definir rotinas de backup, retenção, schedule e filesets

[10] Para mais informações, acesse: https://www.veeam.com/br/vm-backup-recovery-replication-software.html

em máquinas virtuais (VMs). Foi lançado em 2008 e faz parte do *Veeam Availability Suite* (VEEAM. . . ,). Dentre suas funções, destacam-se:

- criar políticas de *backup* flexíveis;
- agendamento de *backups* automatizados;
- monitorar e relatar o status do *backup*;
- executar testes de recuperação;
- recursos de replicação de dados (redundância);
- recuperação rápida.

Para a implantação do plano de *backup*, operamos com o *Veeam Backup and Replication* na versão 12 e licença *Enterprise Plus Edition*.

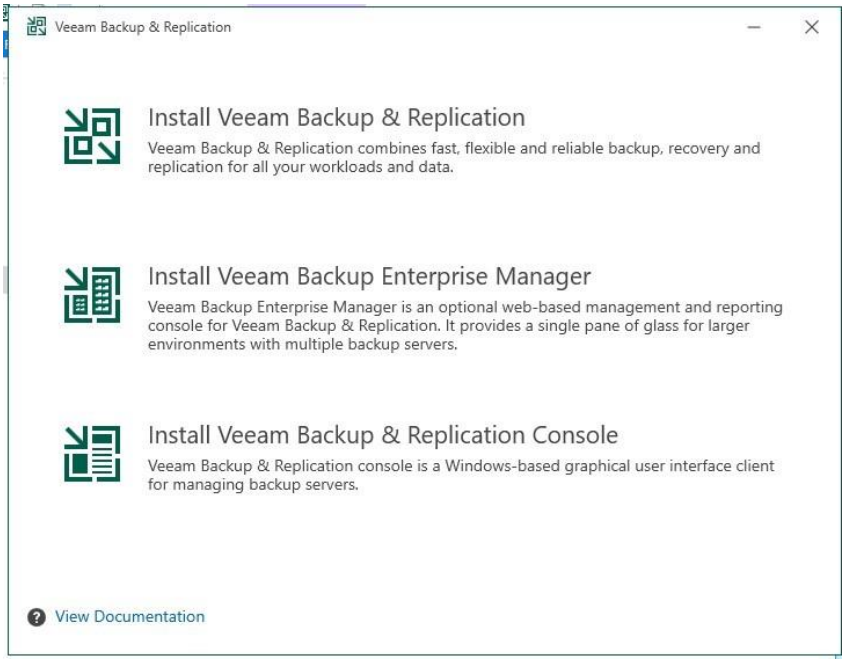
3.4.1.1. Instalação do Veeam Backup & Replication

Primeiro, efetuamos o download no site oficial da *Veeam Backup and Replication*[11]. Para isso, é necessário ter uma conta dentro no site. Depois de logado, basta efetuar o download da ISO.

Em seguida, iniciamos a instalação no servidor ou máquina dedicada, dando dois cliques no *Setup do Veeam* e exibirá os componentes de instalação, como na Figura 6:

[11] Disponível em: https://www.veeam.com/br/vm-backup-recovery-replication-software.html

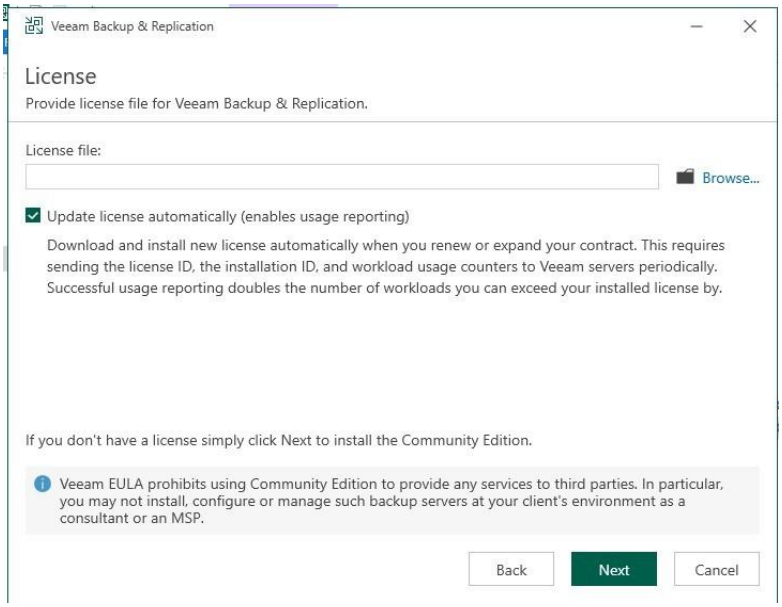
Figura 6 – Janela de instalação



Fonte: Elaborado pelo autor

Após, temos a etapa de licenciamento e os termos de uso precisam serem confirmados. Para utilizar a versão gratuita *(Community Edition)*, basta avançar no botão "*Next* ".

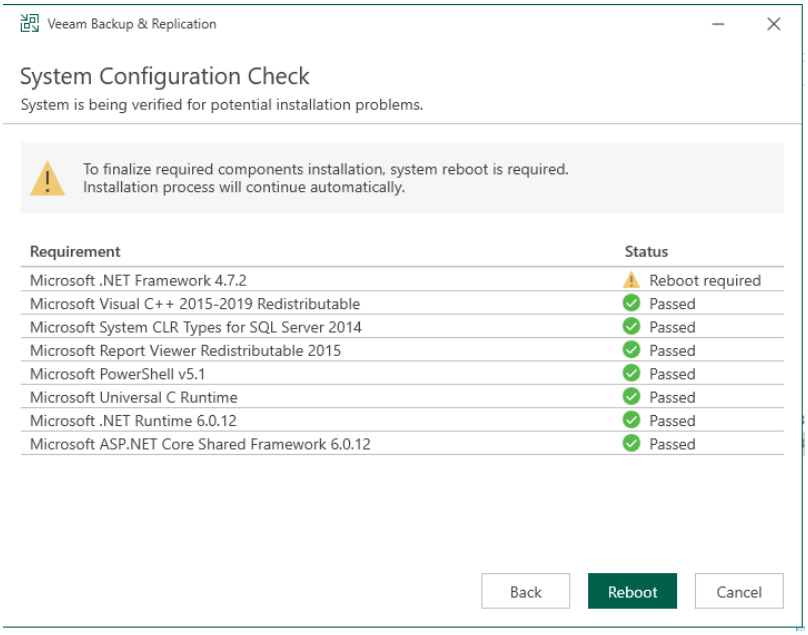
Figura 7 – Janela de licenciamento



Fonte: Elaborado pelo autor

A próxima etapa explana as dependências a nível do sistema operacional. Esses recursos devem ser instalados e são exibidos na tela de checagem de configuração do sistema Figura 8. Caso contrário, ele indica o que deve ser feito.

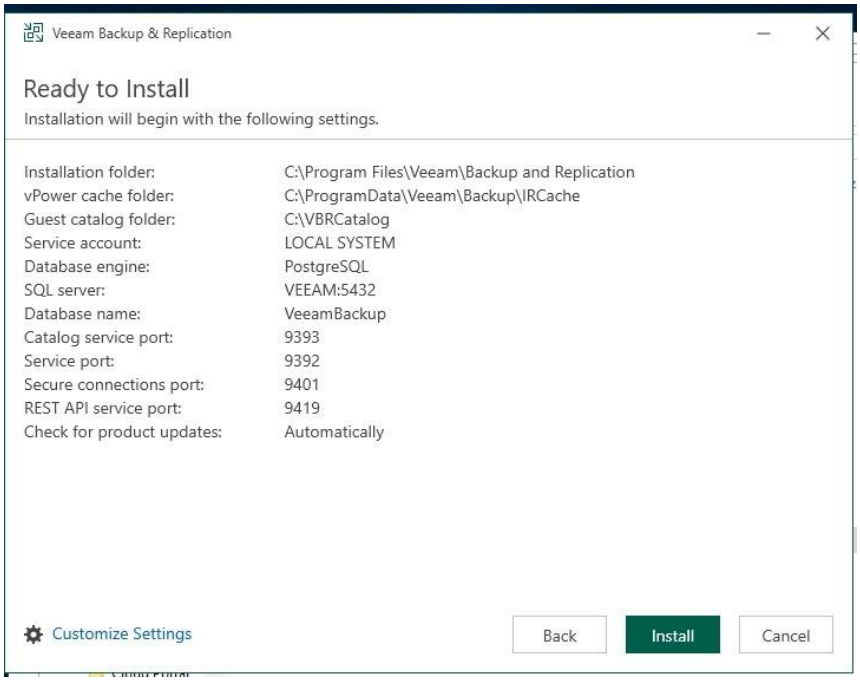
Figura 8 – Janela de checagem



Fonte: Elaborado pelo autor

Após concluída, é exibido o resumo da instalação. Caso necessário a troca de algum dos parâmetros pode ser feita nesse momento, clicando em *"Back"*, como demonstra a Figura 9. Feito isso, é só aguardar sua conclusão.

Figura 9 – Janela de resumo



Fonte: Elaborado pelo autor

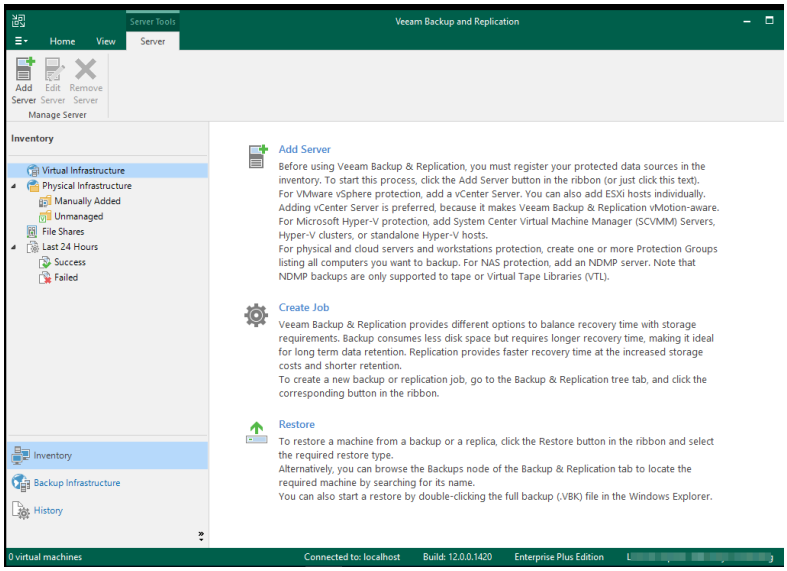
É criado um banco de dados *PostgreSQL*, para armazenar as tarefas de configuração, *backup e replicação*. Após concluída a instalação, executamos o *Veeam* e seguimos para a etapa de configuração.

3.4.1.2. Configuração do Veeam Backup and Replication

Nesta subseção, é demonstrado como designar um ambiente *VMware* para o *Veeam Backup and Replication*.

Na aba Servidor, temos as ferramentas de servidor, onde são apresentadas 3 opções, sendo a adição de um servidor, a criação de um trabalho e restauração, respectivamente:

Figura 10 – Janela de ferramentas

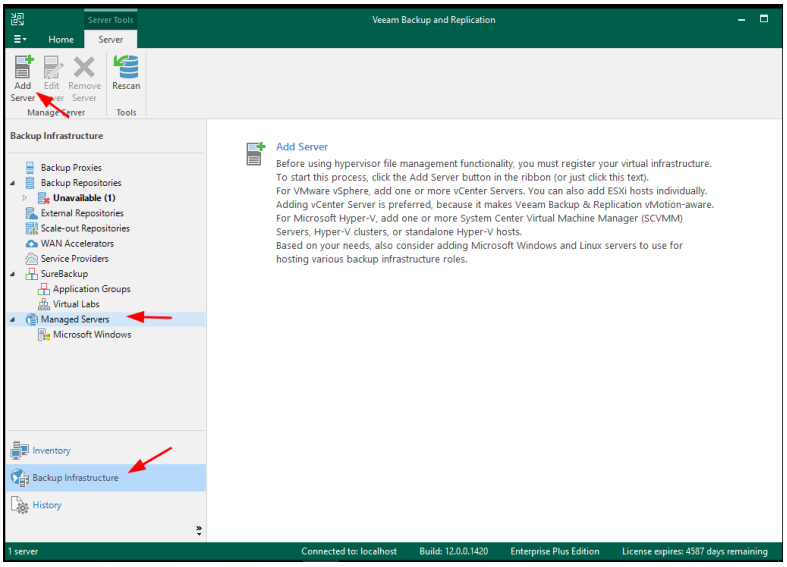


Fonte: Elaborado pelo autor

Para configuração, foram seguidas as etapas:

1. Executamos o console do *Veeam Backup and Replication*;
2. Vamos ao menu *Backup Infrastructure* localizado no menu esquerdo, em seguida, no submenu com o "*Managed Servers*";
3. Assim, iremos adicionar um servidor na opção ("*Add Server*") para conexão ao servidor do *Veeam Backup and Replication*, como abaixo:

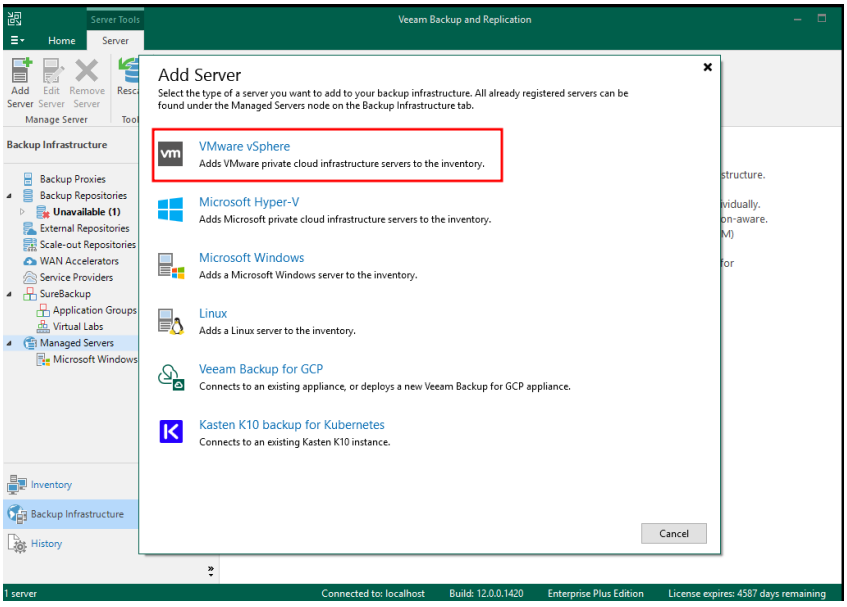
Figura 11 – Adicionar um servidor



Fonte: Elaborado pelo autor

4. Agora é necessário adicionar um host *VMware*, escolhemos a opção "*VMware vSphere*":

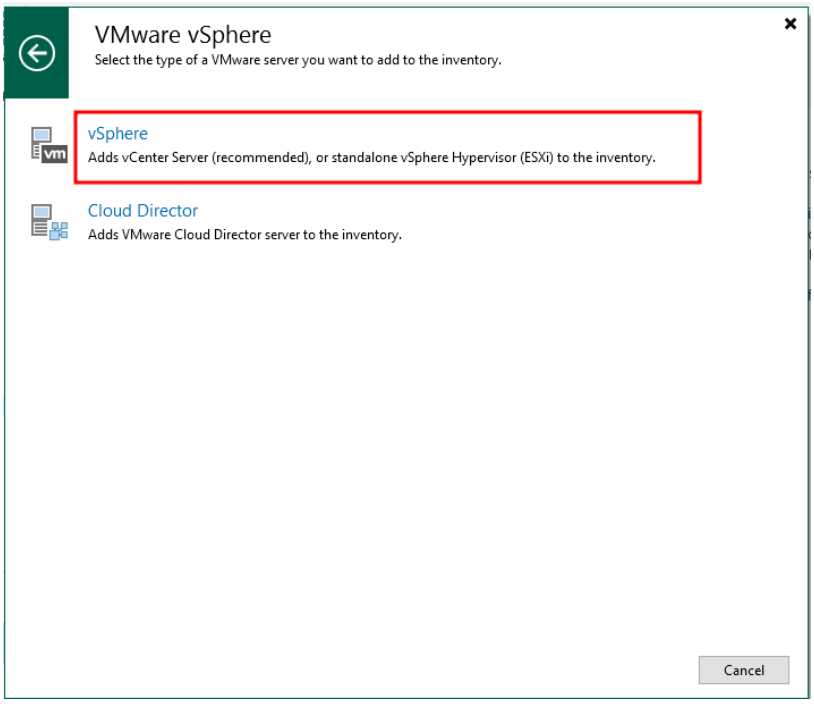
Figura 12 – Adicionar um host



Fonte: Elaborado pelo autor

5. Posteriormente, basta avançarmos clicando na opção "*vSphere*" para inserir o *host ESXi*:

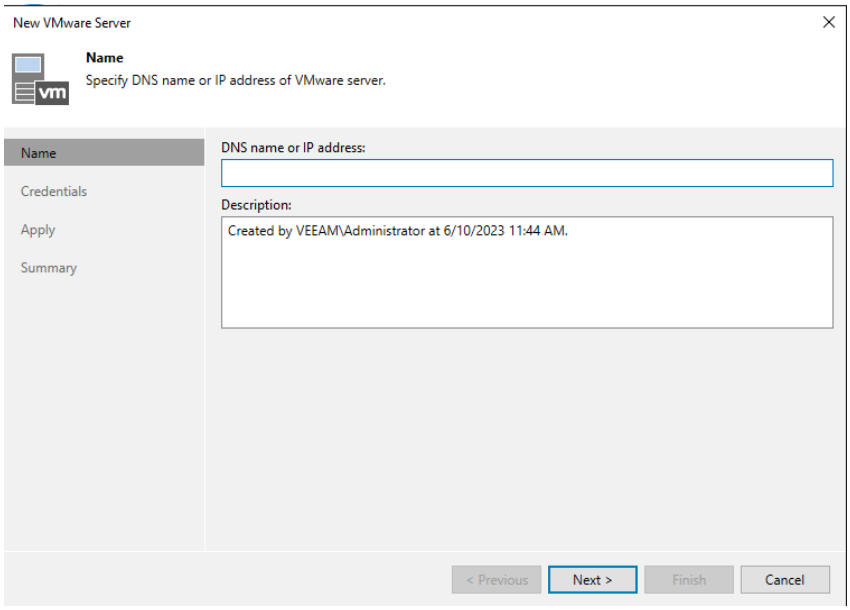
Figura 13 – Adicionar VMware vSphere



Fonte: Elaborado pelo autor

Na tela seguinte, descrevemos as informações do servidor *vCenter* :

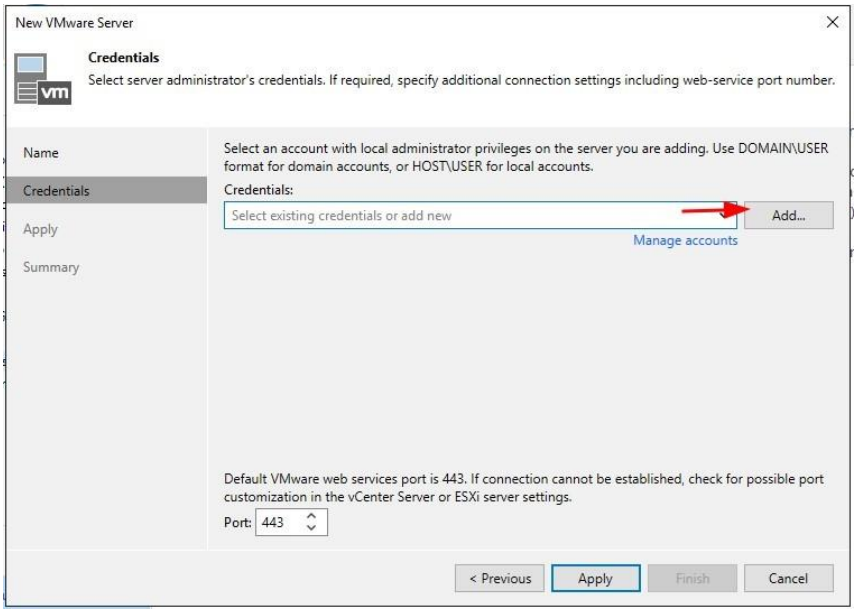
Figura 14 – Nome da VMWare



Fonte: Elaborado pelo autor

No menu abaixo, adicionamos as credenciais do vCenter:

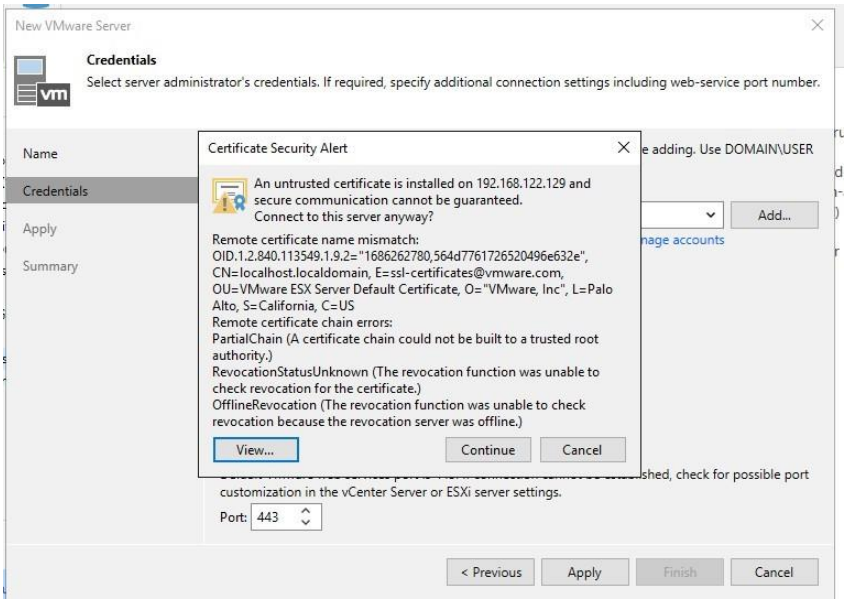
Figura 15 – Credenciais da VMWare



Fonte: Elaborado pelo autor

Feito isso, é solicitado o aceite da conexão com o certificado do vCenter :

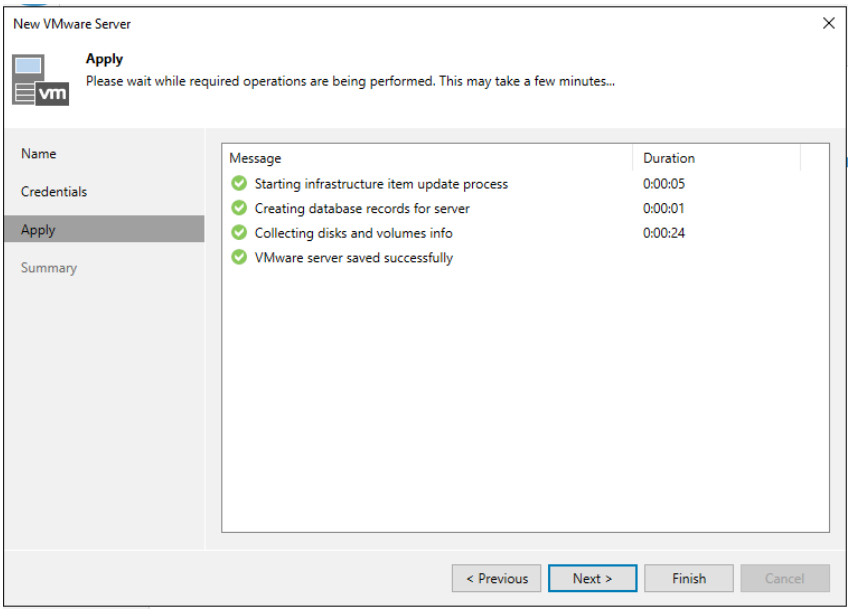
Figura 16 – Certificado de conexão



Fonte: Elaborado pelo autor

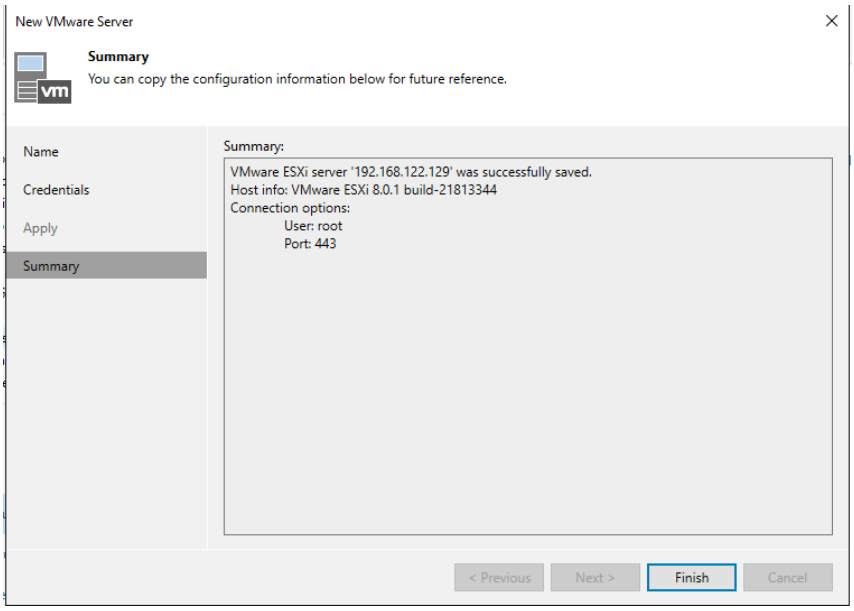
Por conseguinte, a janela abaixo indica algumas validações feitas Figura 17 e se forem bem-sucedidas, as configurações são finalizadas e é só clicar em "*Next*" como na Figura 18.

Figura 17 – Resumo das configurações



Fonte: Elaborado pelo autor

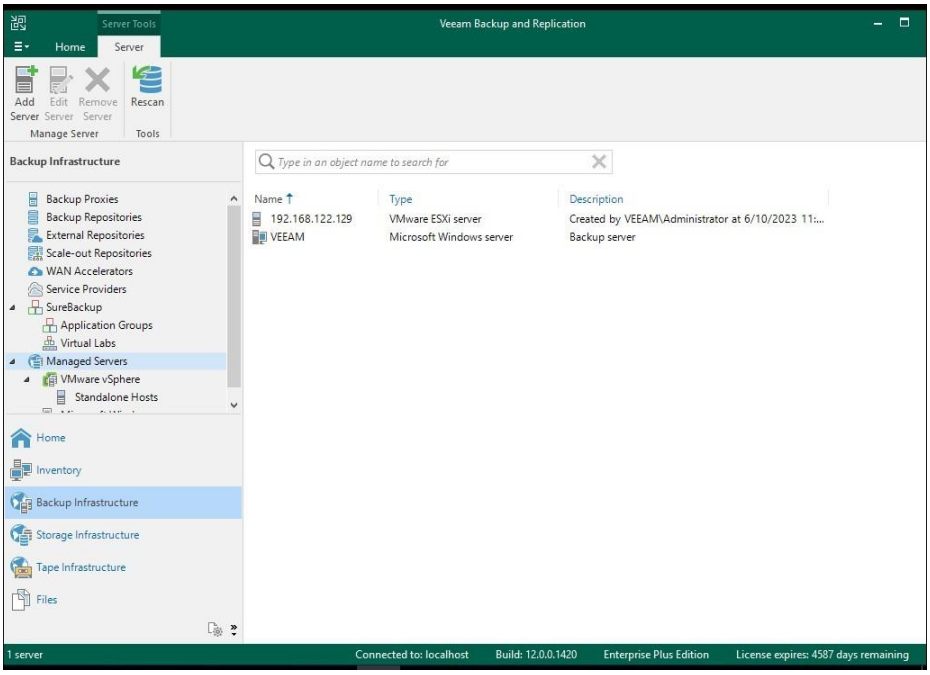
Figura 18 – Resumo das configurações



Fonte: Elaborado pelo autor

Com o fim do processo, podemos exibir os servidores adicionados no menu "*Backup Infrastructure*" e submenu "*Managed Servers*":

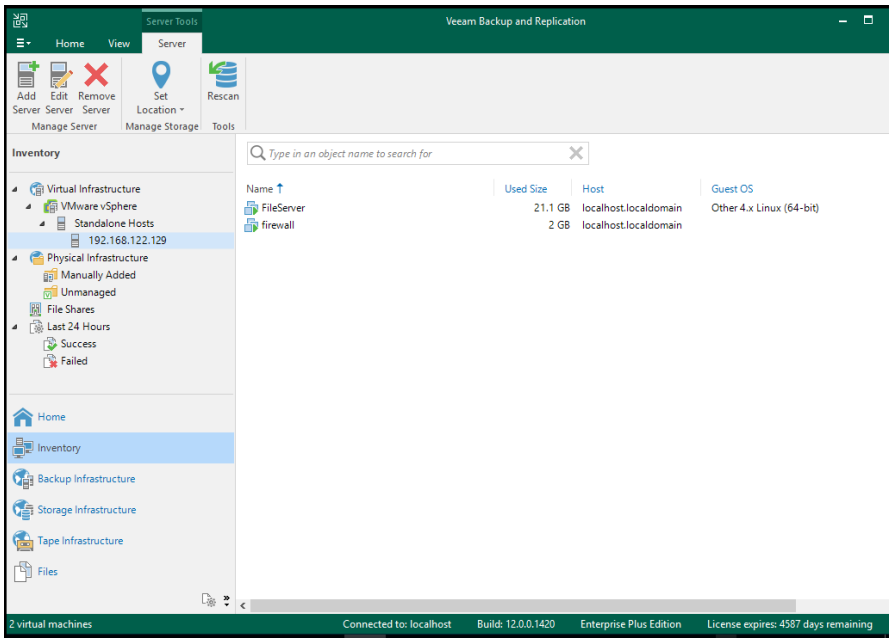
Figura 19 – Servidores criados



Fonte: Elaborado pelo autor

No menu "*Inventory*" e submenu "*VMware vSphere*" são listadas as máquinas virtuais criadas, denominadas como *FileServer* e *Firewall:*

Figura 20 – Máquinas virtuais



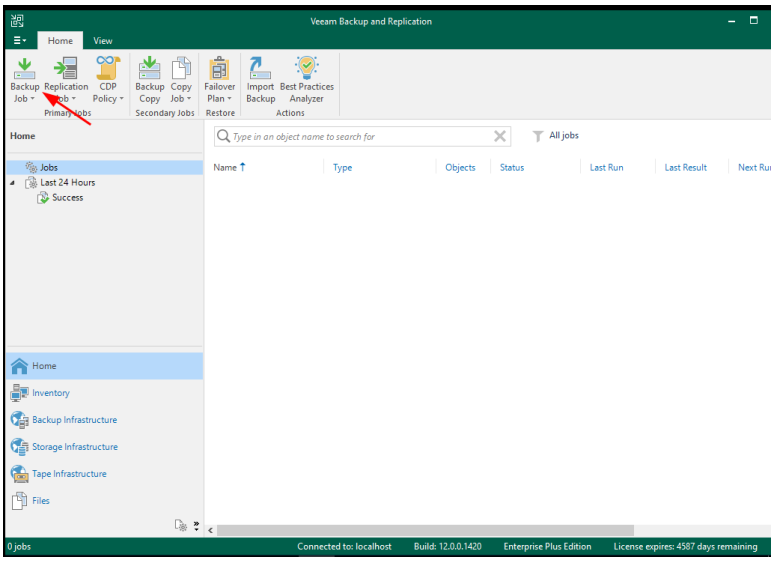
Fonte: Elaborado pelo autor

3.4.2. O processo de backup

O próximo tópico é a configuração de uma tarefa, também conhecida como "job". Para isso, são elencados os seguintes passos:

1. No menu "*Home*" escolhemos a opção *"Backup Job"* para criar um novo trabalho, como abaixo:

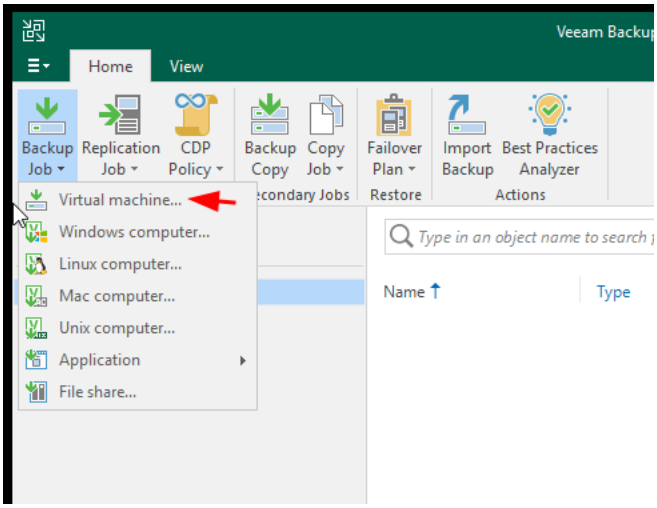
Figura 21 – Criando job de backup



Fonte: Elaborado pelo autor

Após, escolhemos a opção "*Virtual Machine"*:

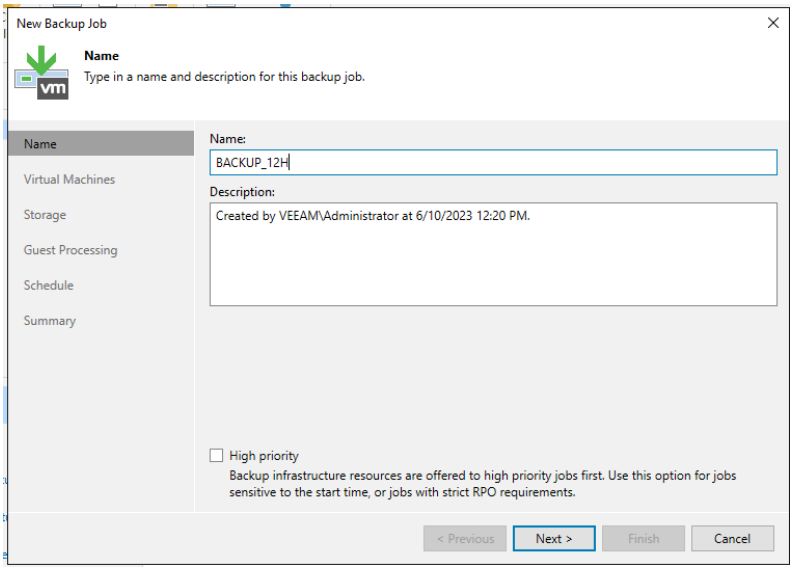
Figura 22 – Máquinas virtuais



Fonte: Elaborado pelo autor

2. Com isso, é exposta uma janela de configuração para a tarefa onde será definido o nome do *job* e sua descrição. Neste trabalho, o nome especificado foi *"Backup_12H"* e a descrição padrão. Logo após, avançamos para a próxima etapa clicando em *"Next"*:

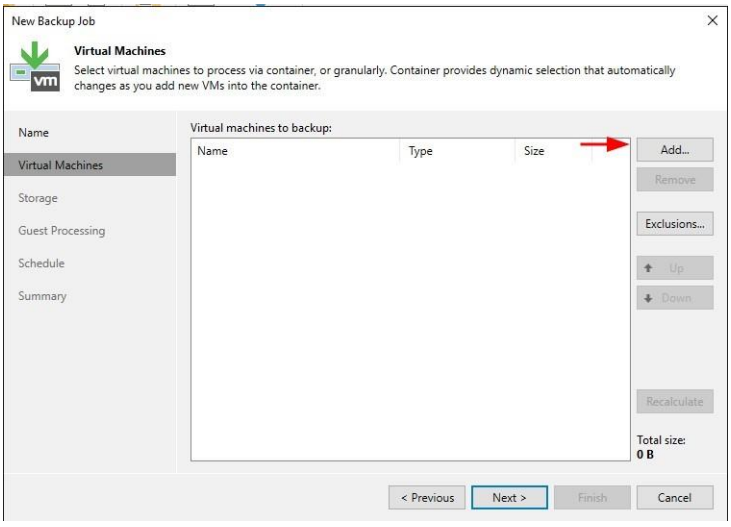
Figura 23 – Máquinas virtuais



Fonte: Elaborado pelo autor

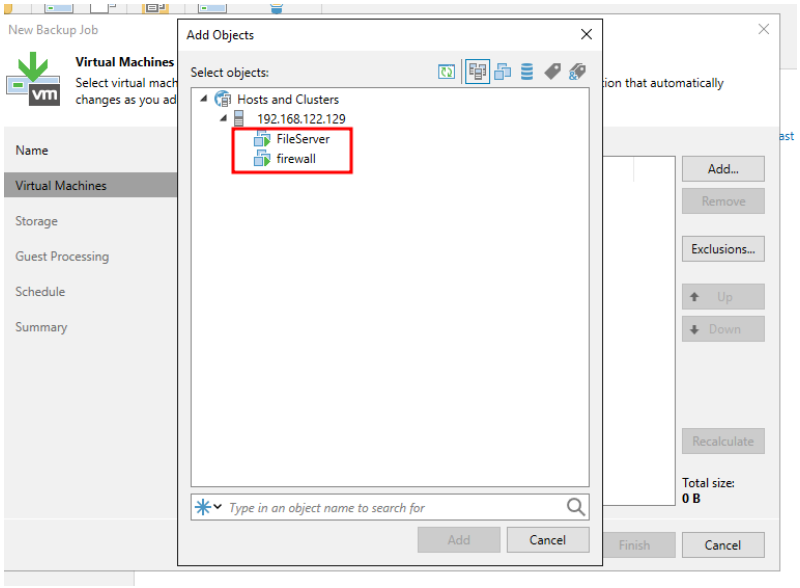
3. Agora, adicionamos a máquina virtual clicando no botão *"Add"* (Figura 24) e selecionamos as VMs, como na Figura 25:

Figura 24 – Adicionando máquinas virtuais



Fonte: Elaborado pelo autor

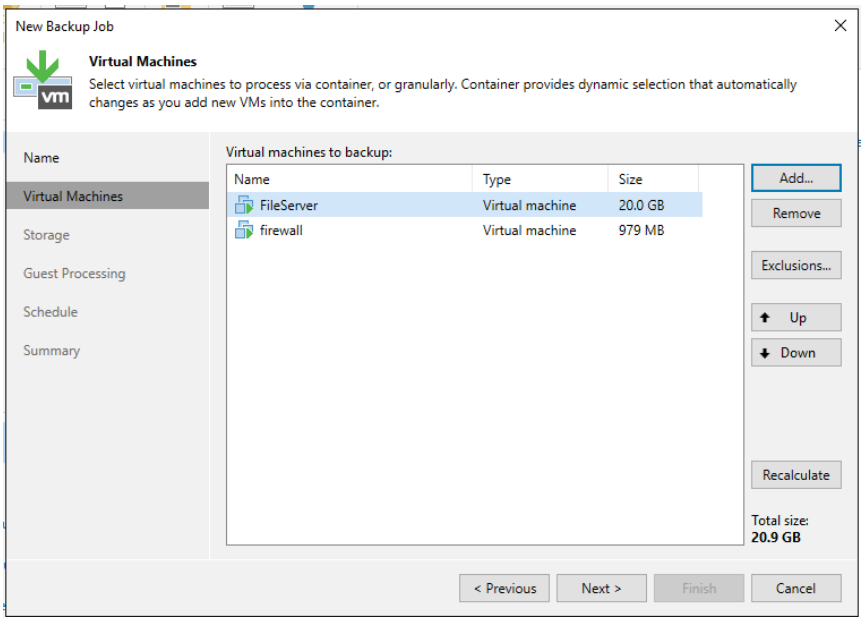
Figura 25 – Selecionando máquinas virtuais



Fonte: Elaborado pelo autor

Dessa maneira, é possível ver a listagem das máquinas virtuais que serão processadas pelo *job* de *backup*:

Figura 26 – Lista de máquinas virtuais

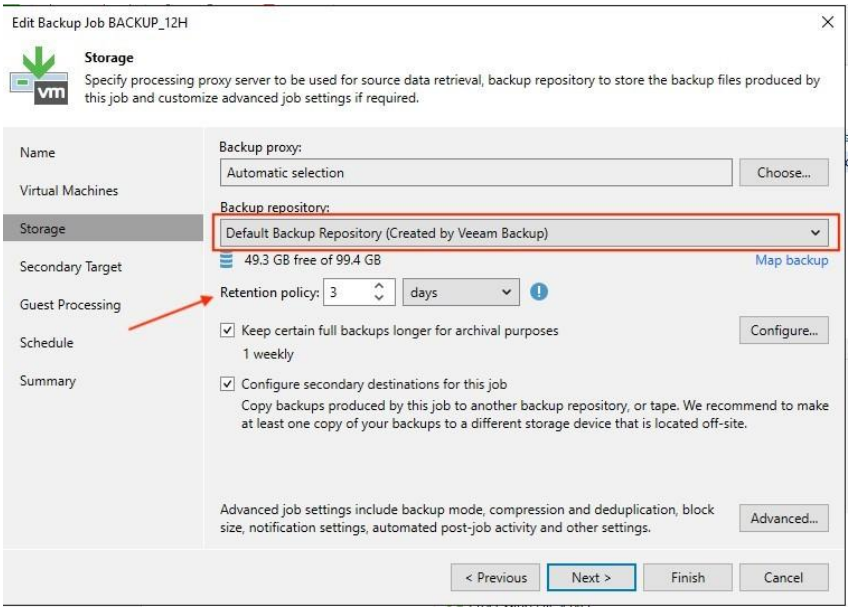


Fonte: Elaborado pelo autor

Uma tarefa ou (*job*) pode conter várias VMs para executar um *backup*. Nesta situação, temos 2 VMs, cada uma com um total de 20,9GB.

4. Partindo para a etapa subsequente, configuramos o armazenamento definindo o repositório e sua retenção (pontos de restauração), como em Figura 27. A estratégia adotada foi o repositório local do *Veeam* que é configurado no ato da instalação. Além disso, a *"retention policy"* foi setada para 2 dias, ou seja, serão gerados 2 arquivos de *backup* e quando houver um processo de *restore*, há a possibilidade de restaurar esses pontos.

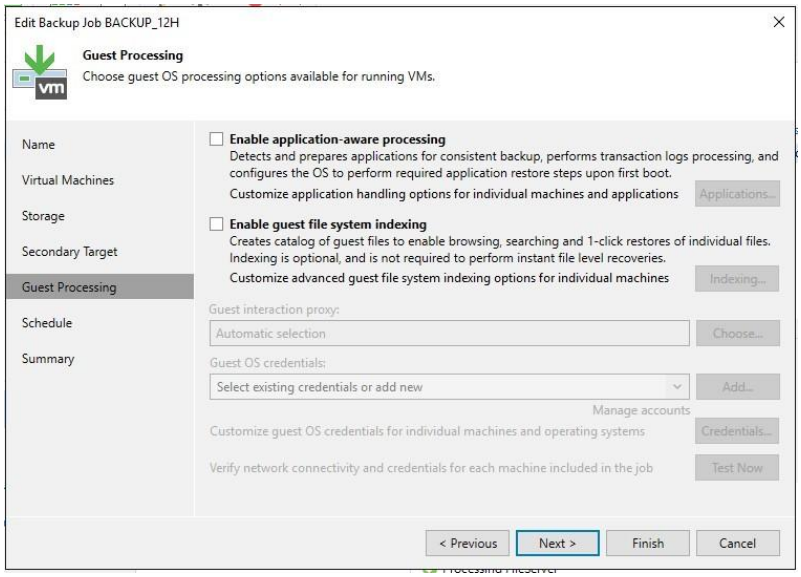
Figura 27 – Configuração do armazenamento



Fonte: Elaborado pelo autor

5. Na fase seguinte, existem as opções *"Enable application-aware processing"* e *"Enable guest file system indexing"*. São configurações avançadas unicamente para processamento com reconhecimento de aplicativos e índice do sistema de arquivos convidado, respectivamente. Para máquinas de *Active Directory* (AD) é importante habilitar a opção *"Enable application-aware processing"*:

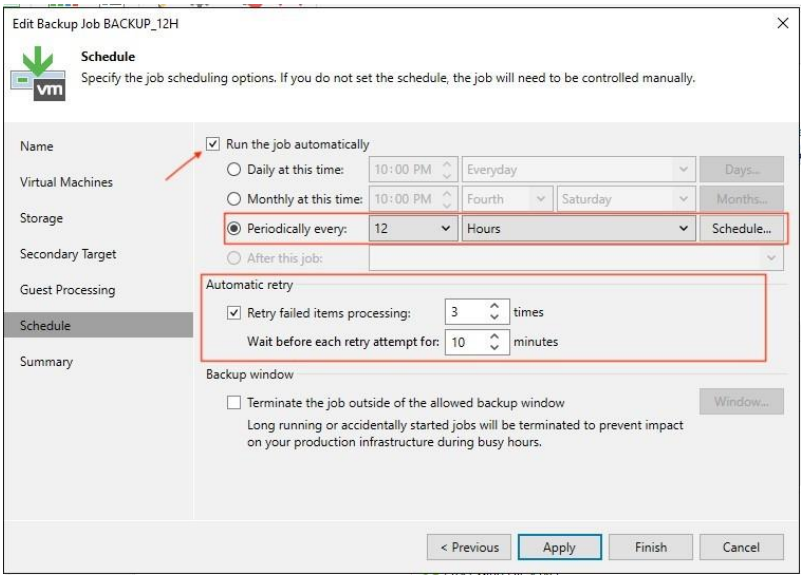
Figura 28 – Configurações avançadas



Fonte: Elaborado pelo autor

6. Seguindo, configuramos o *schedule* ou programação da execução do *backup*. Nesse quesito, podem ser especificados diversos tipos de agendamentos como: diário, mensal, em dias ou horários específicos. Neste cenário, habilitamos a execução automática da tarefa, com periodicidade a cada 12hs e com *"automatic retry"* (configuração padrão) que significa que são feitas 3 tentativas em um intervalo de 10 minutos em caso de falha na execução do *job* de *backup*:

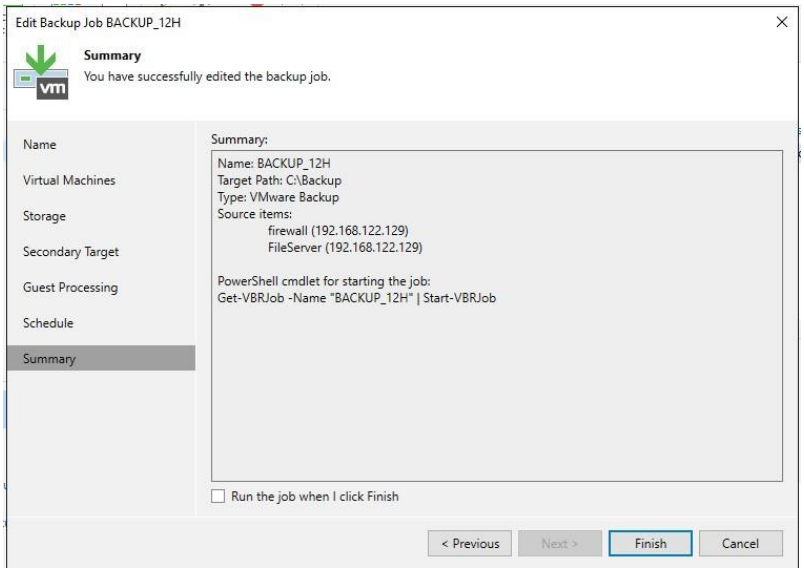
Figura 29 – Programação do backup



Fonte: Elaborado pelo autor

7. Ao clicar em *"Apply"* temos o resumo do *job* de *backup* configurado. Após, executamos o *job* clicando em *"Finish"*:

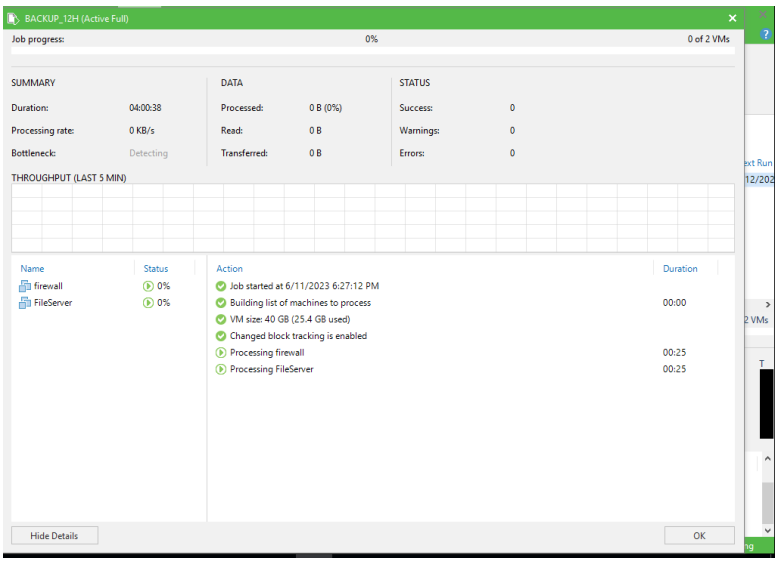
Figura 30 – Programação do backup



Fonte: Elaborado pelo autor

8. Com isso, observamos o menu *"Running"* executando no console e sua porcentagem de execução:

Figura 31 – Execução do job de backup



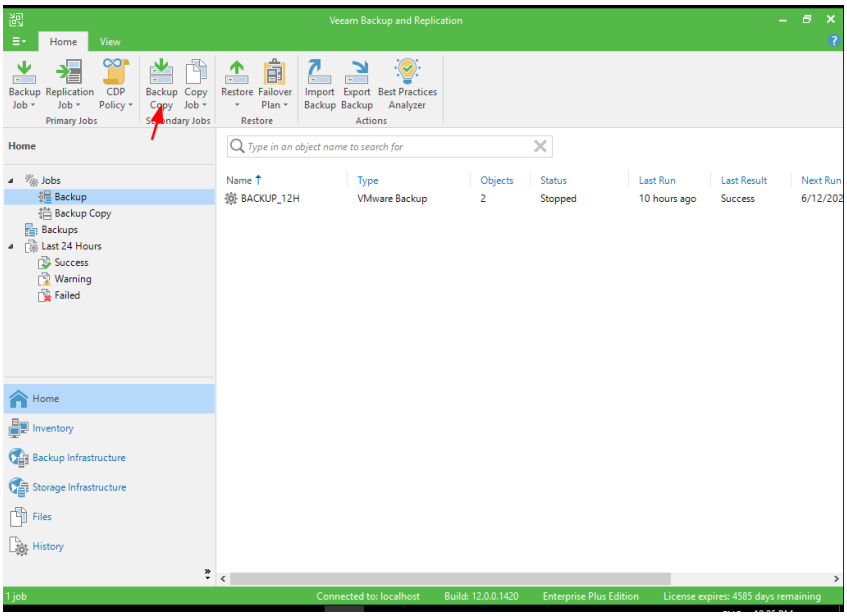
Fonte: Elaborado pelo autor

3.4.2.1. Modo de cópia de backup

Após seguir as etapas do assistente para configurar o job e programar sua execução, criaremos uma cópia do backup que tem finalidade de criar pontos de restauração ou backups.

1. No console, vamos até a opção "Backup Copy":

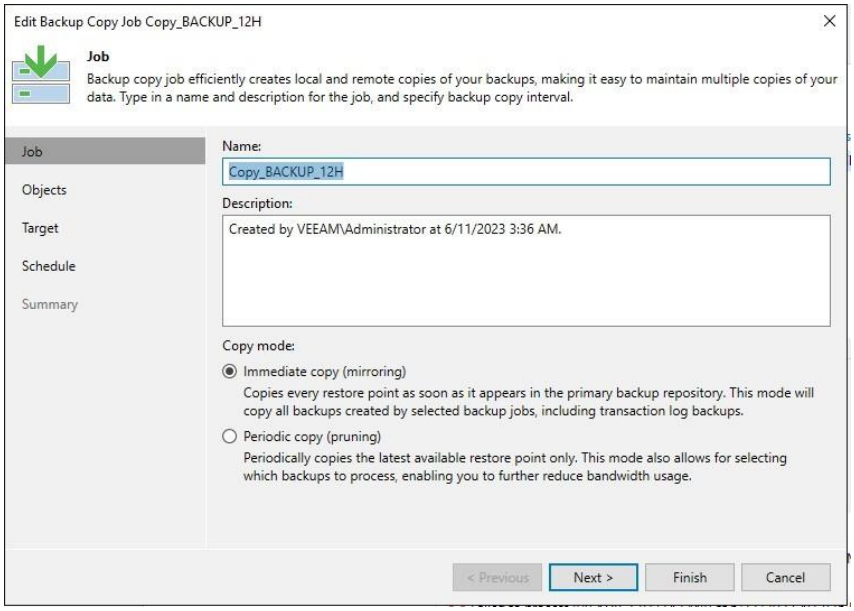
Figura 32 – Cópia do backup



Fonte: Elaborado pelo autor

2. Na tela seguinte, é pedido as especificações para o trabalho de cópia de backup, como nome e descrição. O modo de cópia de segurança é a "Immediate copy" que copia novos pontos de restauração a cada backup:

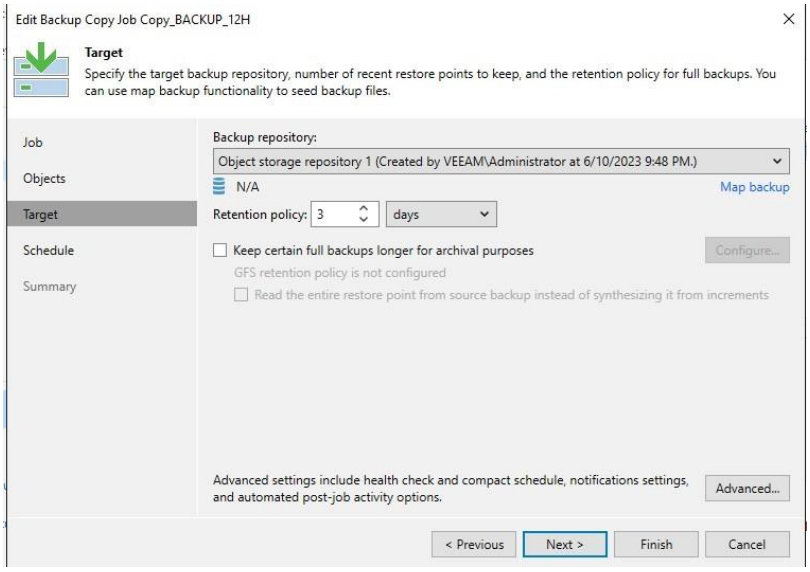
Figura 33 – Cópia do backup



Fonte: Elaborado pelo autor

3. A Figura 34 mostra o local do repositório do *backup* e a política de retenção configurada para 3 dias:

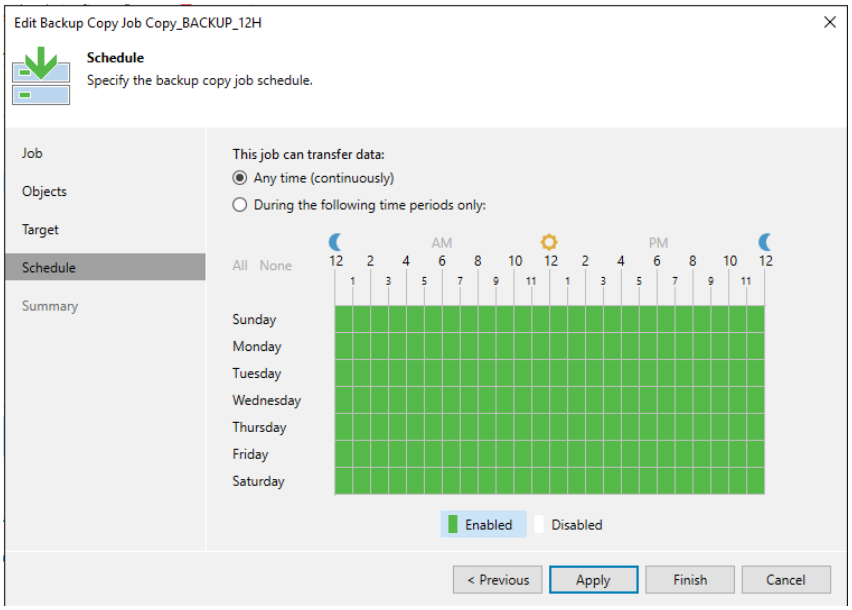
Figura 34 – Retenção do backup



Fonte: Elaborado pelo autor

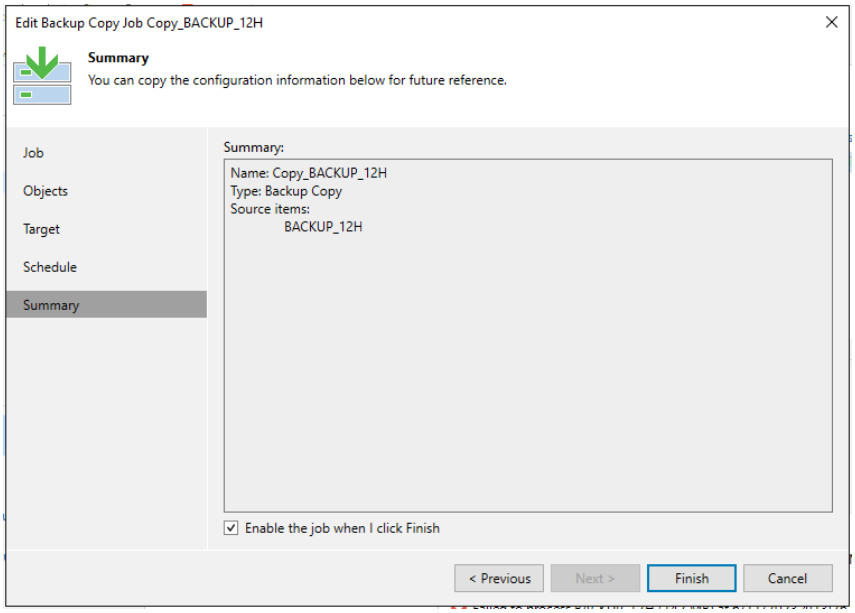
4. Para programação do *job* de cópia, foi escolhido o modo contínuo, como em Figura 35. Após, é exibido o resumo das configurações e finalizado o procedimento, como representa Figura 36.

Figura 35 – Programação do job para cópia do backup



Fonte: Elaborado pelo autor

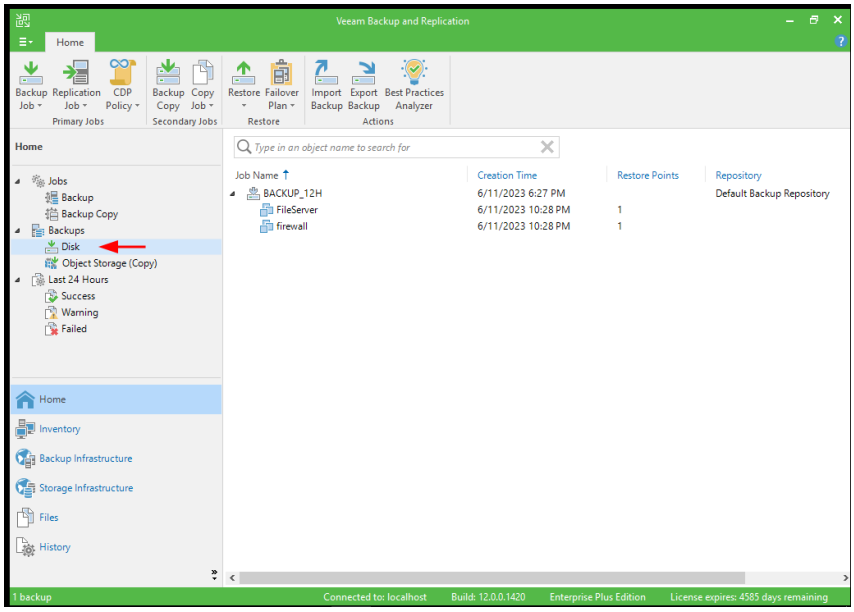
Figura 36 – Resumo das configurações de cópia do backup



Fonte: Elaborado pelo autor

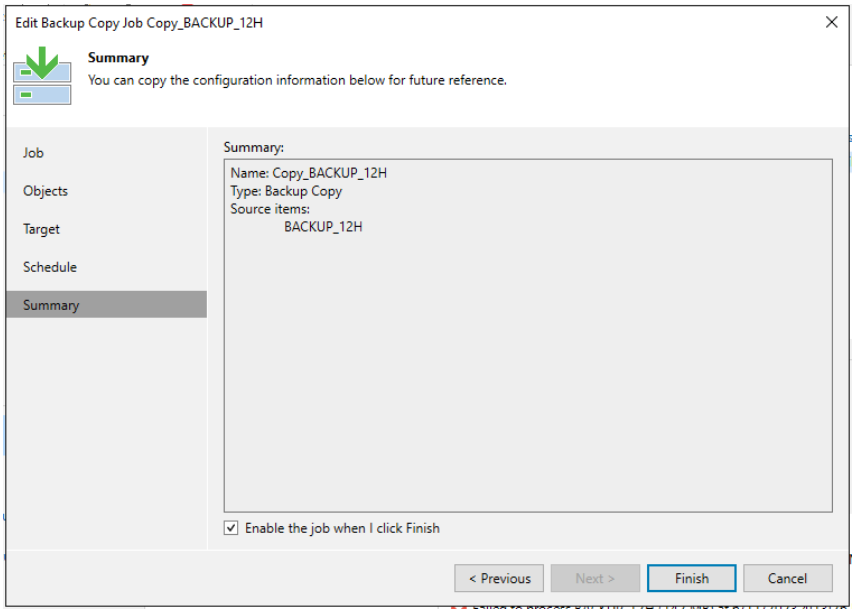
A seguir, são exibidos os jobs de backup configurados para as 2 VMs. Sendo a Figura 37 demonstrando o job programado a cada 12hs e a Figura 38, a cópia do backup:

Figura 37 – Job de backup 12 hs



Fonte: Elaborado pelo autor

Figura 38 – Cópia do backup

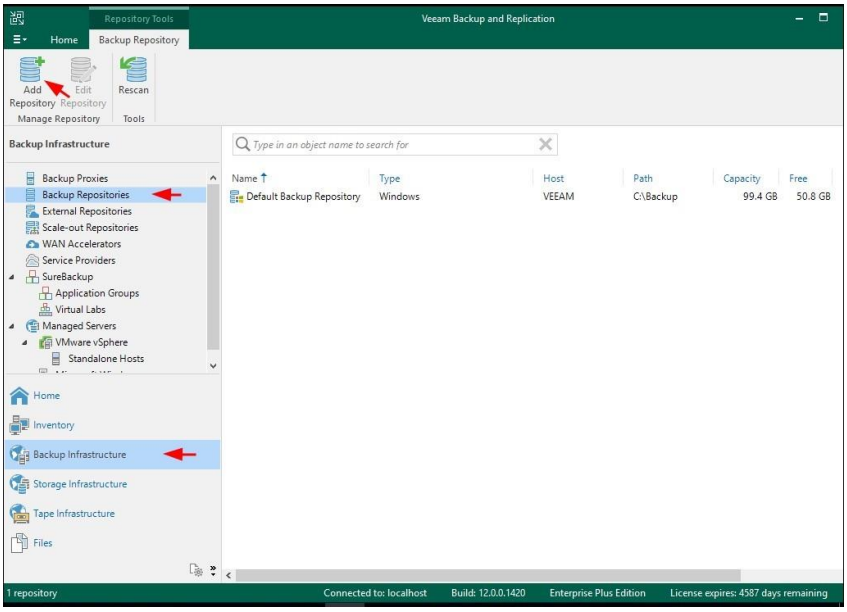


Fonte: Elaborado pelo autor

3.4.3. Configuração do Veeam no Google Cloud Storage

Na região "*Backup Infrastructure"* e menu "*Backup Repositores*", adicionamos um repositório de *backup*:

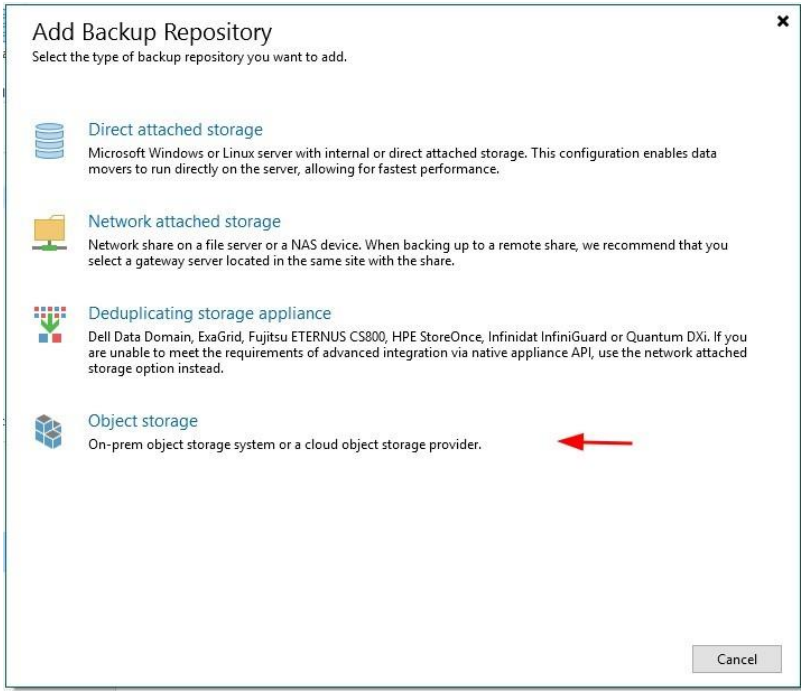
Figura 39 – Adição de repositório de backup



Fonte: Elaborado pelo autor

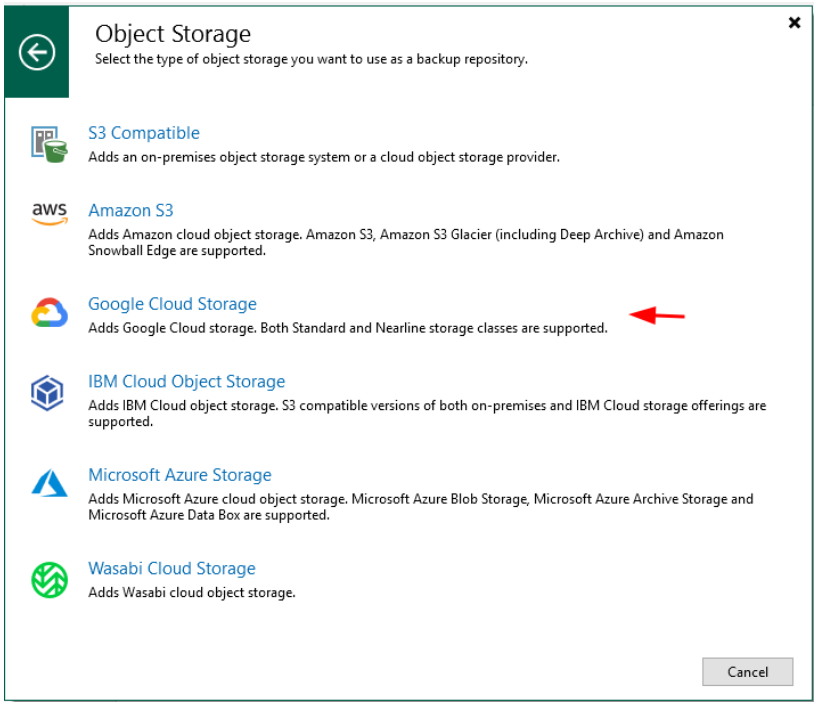
Selecionamos a alternativa "*Object storage*" como a Figura 40 e a escolha da nuvem a ser utilizada, no caso abordado é a "*Google Cloud Storage*", como mostra a Figura 41:

Figura 40 – Objeto de armazenamento



Fonte: Elaborado pelo autor

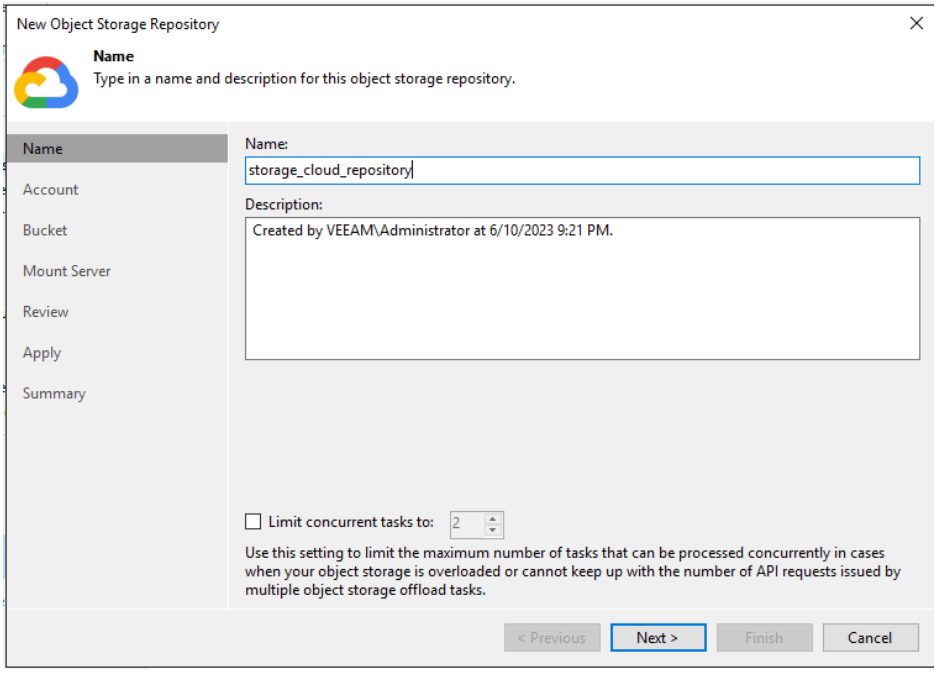
Figura 41 – Escolha do armazenamento em nuvem



Fonte: Elaborado pelo autor

Inserimos um nome e descrição nos campos abaixo:

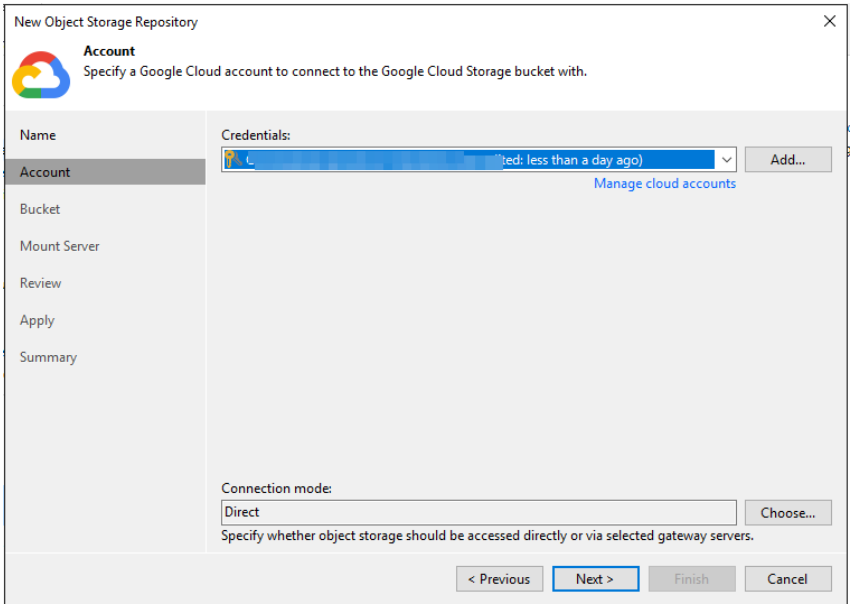
Figura 42 – Nome e descrição do objeto de repositório



Fonte: Elaborado pelo autor

Selecionamos as credencias para conexão com o Google Bucket :

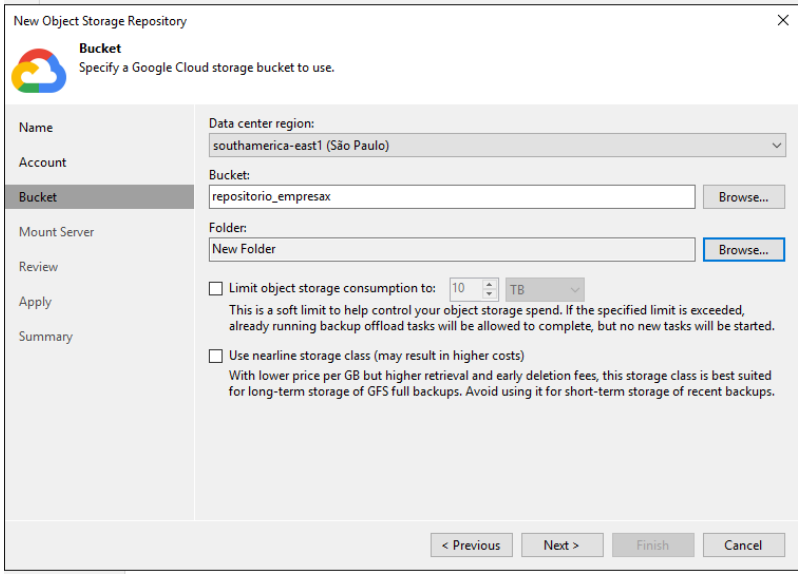
Figura 43 – Conexão com o Google Bucket



Fonte: Elaborado pelo autor

Selecionamos a região do datacenter, o bucket e a pasta a ser utilizada:

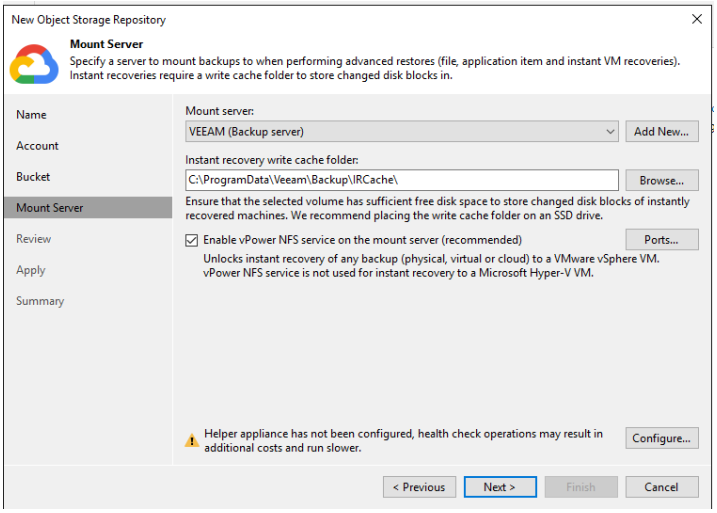
Figura 44 – Configuração do Google Bucket



Fonte: Elaborado pelo autor

Após, temos a etapa de montar o servidor, onde é especificado o servidor usado como servidor de montagem cabível em processo de restauração. Abaixo, selecionamos uma pasta usada para gravar o cache das operações. Por último, na caixa de seleção, ativamos o repositório de backup para ser acessível pelo serviço *Veeam vPower* NFS:

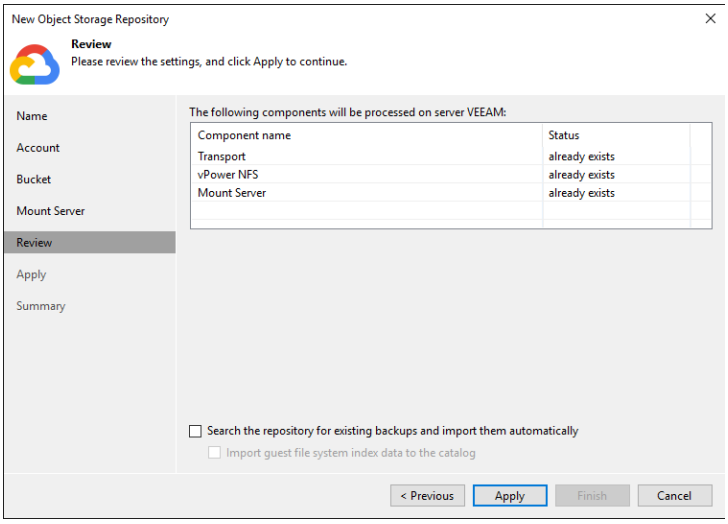
Figura 45 – Montagem de servidor



Fonte: Elaborado pelo autor

Seguindo, a tela de "*Review*" é exibida com as configurações a serem aplicadas:

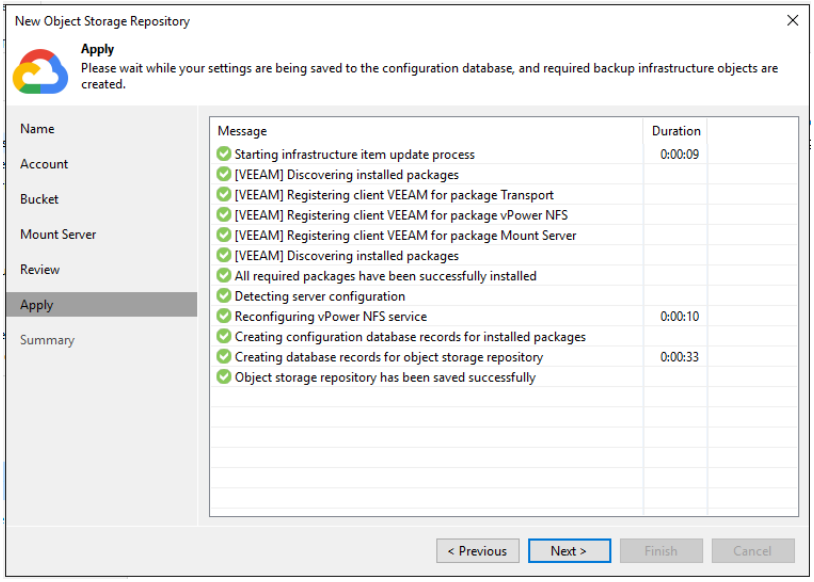
Figura 46 – Revisão de montagem de servidor



Fonte: Elaborado pelo autor

E, posteriormente, o sucesso ou falha do que foi aplicado na seção "*Apply*":

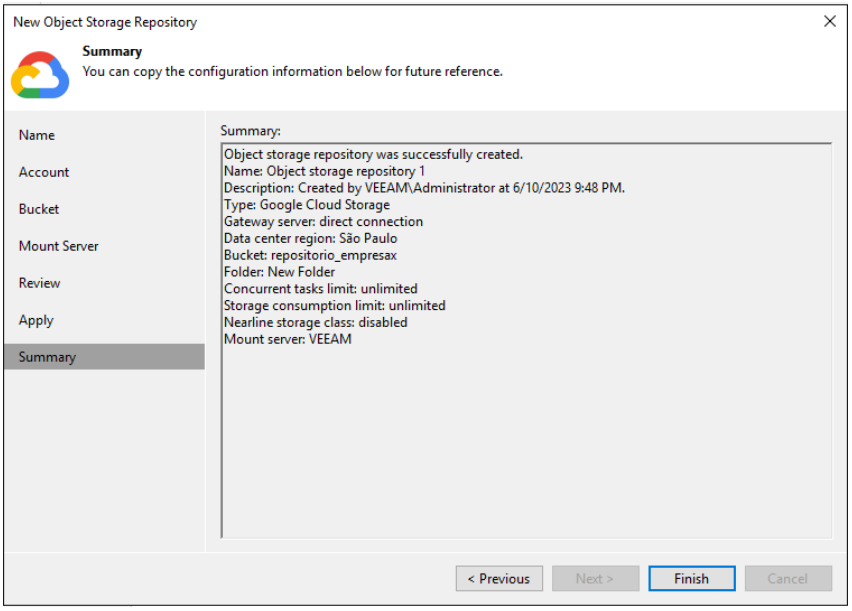
Figura 47 – Objetos aplicados



Fonte: Elaborado pelo autor

Na imagem a seguir, constatamos a integração bem-sucedida do objeto de repositório no *Google Cloud Storage*:

Figura 48 – Objetos aplicados

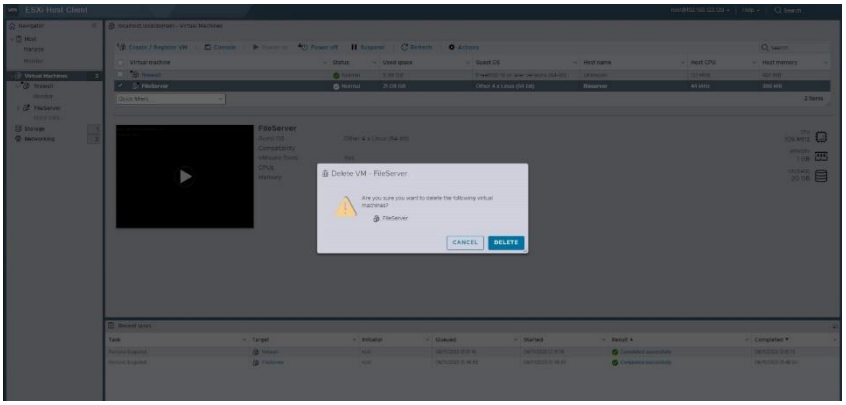


Fonte: Elaborado pelo autor

3.5. TESTES DE RESTORE E VALIDAÇÃO DA INFRAESTRUTURA

Uma vez executado o processo de backup, excluiremos a VM "*FileServer"*:

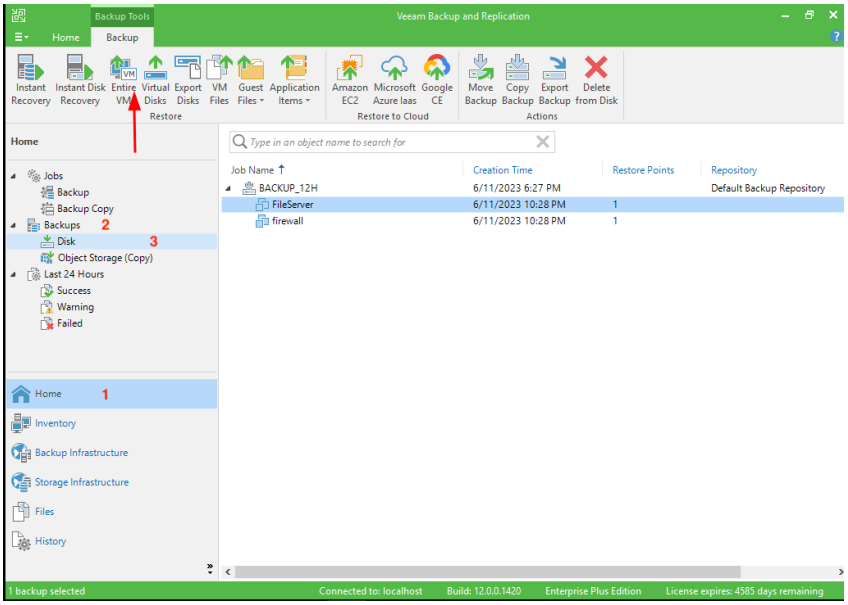
Figura 49 – Exclusão da VM FileServer



Fonte: Elaborado pelo autor

De volta ao console do *Veeam*, abrimos o menu "*Home*" e depois "*Backups*" > "*Disk*", escolhendo a opção "*Entire VM*" disposta na barra acima:

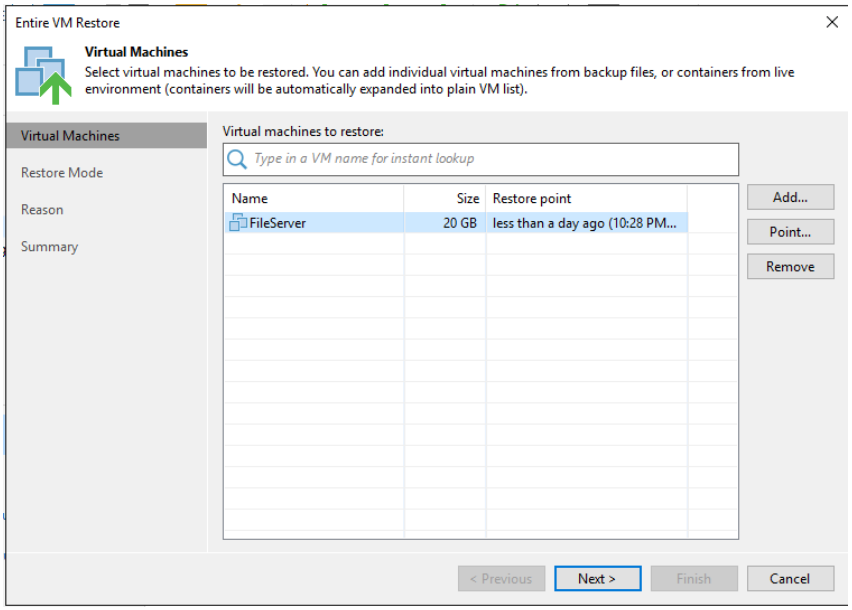
Figura 50 – Menu de recuperação da VM



Fonte: Elaborado pelo autor

O processo de restauração da VM se inicia e apresenta a VM excluída anteriormente ("*FileServer*"):

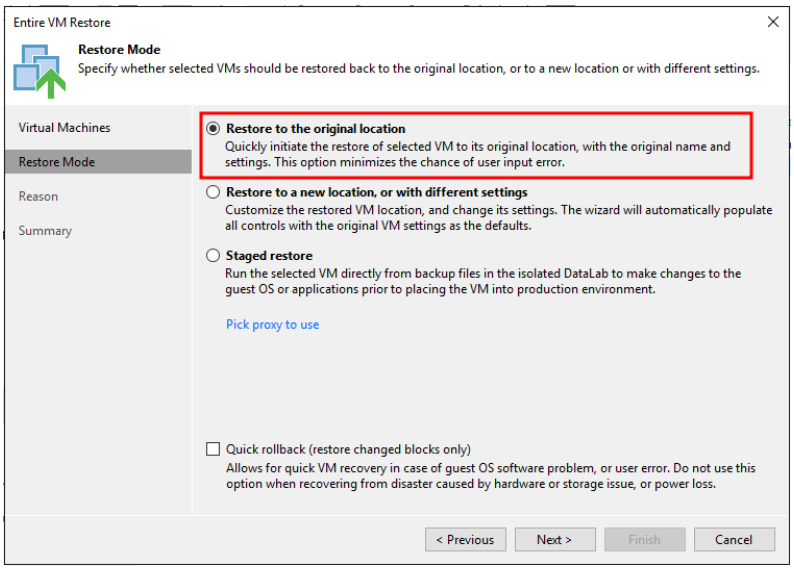
Figura 51 – VM FileServer



Fonte: Elaborado pelo autor

Após, iniciamos o modo de restauração para a localização de origem:

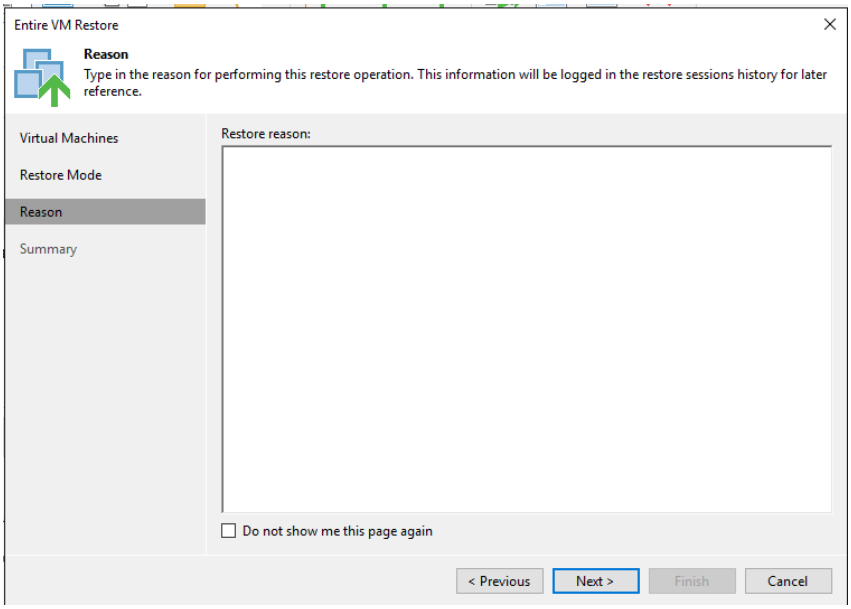
Figura 52 – Localização da restauração



Fonte: Elaborado pelo autor

Na seção razão da restauração ou "*Restore reason*", avançamos com o botão "*Next*":

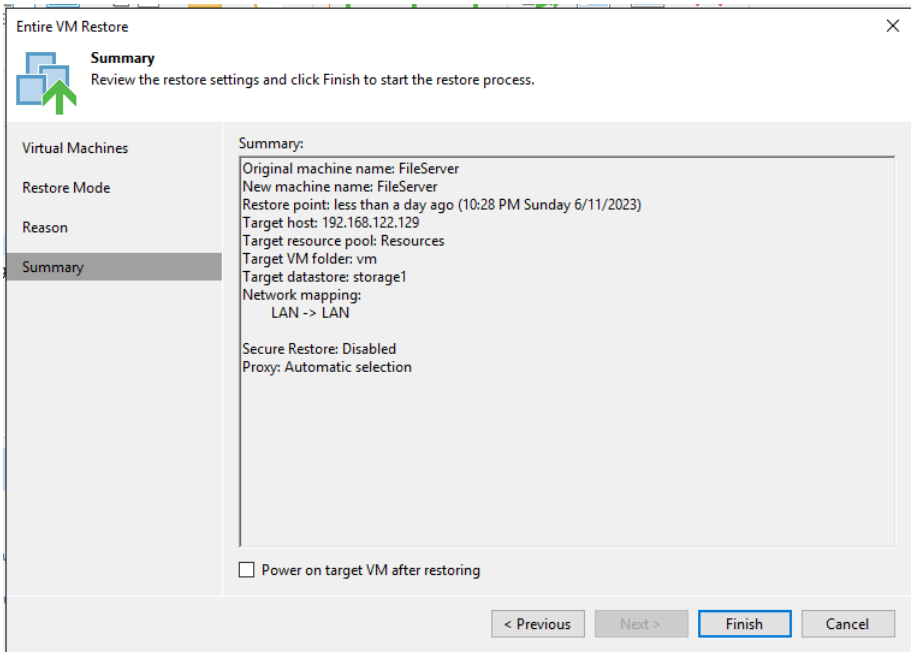
Figura 53 – Razão da restauração



Fonte: Elaborado pelo autor

E obtemos então, o resumo de restauração:

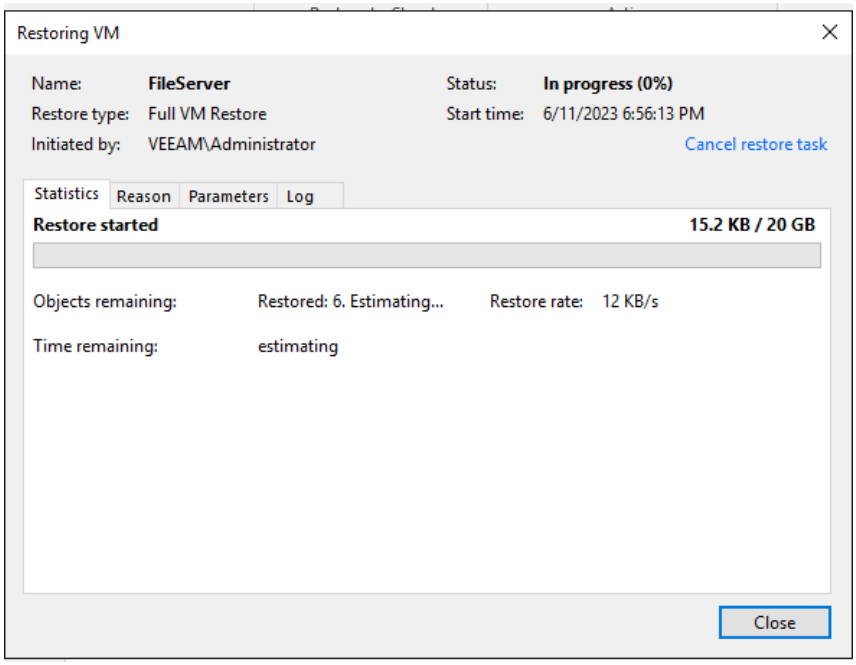
Figura 54 – Resumo da restauração



Fonte: Elaborado pelo autor

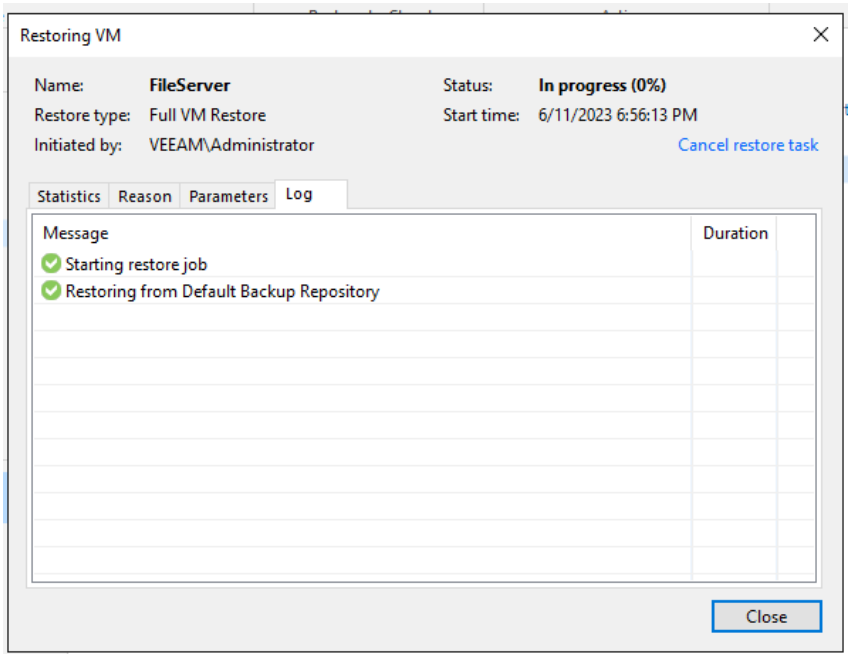
A seguir, temos o processo de restauração da VM "*FileServer*", estatísticas e a aba de *Logs,* indicando mensagem de sucesso:

Figura 55 – Estatísticas da restauração



Fonte: Elaborado pelo autor

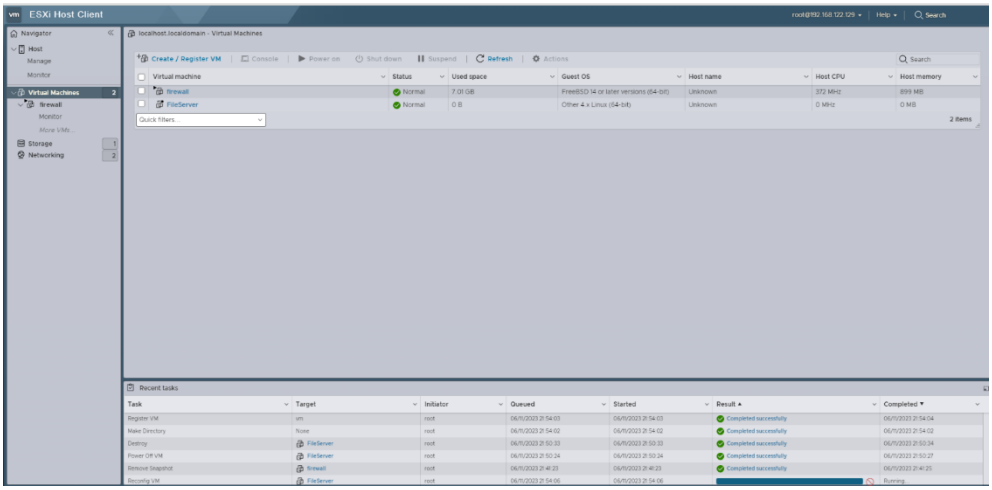
Figura 56 – Logs da restauração



Fonte: Elaborado pelo autor

Como validação final, temos a VM restaurada no ambiente original:

Figura 57 – Validação da restauração



Fonte: Elaborado pelo autor

4. RESULTADOS

Após exposição dos motivos para implementação de uma infraestrutura de *backup*, é plausível considerar sua extrema importância, pois visa garantir a disponibilidade, integridade e segurança de dados. Em detrimento disso, torna-se tácito destacar os aspectos prós e contras no que tange às ferramentas, tipos de *backup*, uso de máquinas virtuais, armazenamento em provedores de nuvem e técnicas de recuperação de desastres.

Com o grande crescimento dos dados, mecanismos de armazenamento de informações estão em voga. A nuvem pública tem capacidade para armazenar grandes quantidades de informações, eliminando a necessidade de uma grande infraestrutura local. Requer baixo custo de instalação e manutenção em comparação a outros mecanismos de armazenamento. No que concerne aos custos, os valores dependem da região, do tipo de armazenamento e quantidade de dados.

Diante disso, é válido mencionar o software *Veeam Backup and Replication* como uma das melhores e mais conhecidas soluções para backup e recuperação de dados. Disponibiliza uma interface intuitiva, execução dos variados tipos de *backup* visando atender às características específicas de cada ambiente, como *backup* de máquinas virtuais (VM) e captura completa de sistemas operacionais, aplicativos e dados. Ocasionando assim, na eficaz restauração de dados independente da causa, reduzindo o tempo de inatividade e impacto, tal como integração com nuvens públicas disponíveis no mercado, sendo alternativa flexível, segura e escalável para o armazenamento. Em contrapartida, os aspectos negativos da solução baseiam-se nos custos associado ao licenciamento e na manipulação da mesma, por exigir conhecimentos técnicos específicos para configuração adequada.

Na empresa X, foi empregada a infraestrutura de backup com o software *Veeam Backup and Replication*, realizada sua configuração, periodicidade, retenção e localização. De acordo com os testes de recuperação realizados, a VM *FileServer* teve recuperação bem-sucedida

em sua totalidade após sua exclusão, o envio para nuvem permitiu rapidez e segurança das informações. As estimativas de custos do *software* apresentam-se no valor de 33 mil reais com licença de 5 anos na edição (*Enterprise Plus Edition*) e a hospedagem no provedor de nuvem *Google Cloud* em ambiente simulado de 100GB foi de R$ 18,50 por mês, sendo o cálculo avaliado de acordo com a quantidade de armazenamento provisionada.

5. CONSIDERAÇÕES FINAIS

A implementação adequada de um backup é essencial para garantir a disponibilidade contínua dos dados e a recuperação em casos de perda ou desastres. Ao seguir as melhores práticas, como definir políticas de *backup*, escolher a estratégia correta, armazenar os backups de forma segura, criptografar os dados e realizar testes de *restore,* é possível garantir a eficácia e a segurança dos backups.

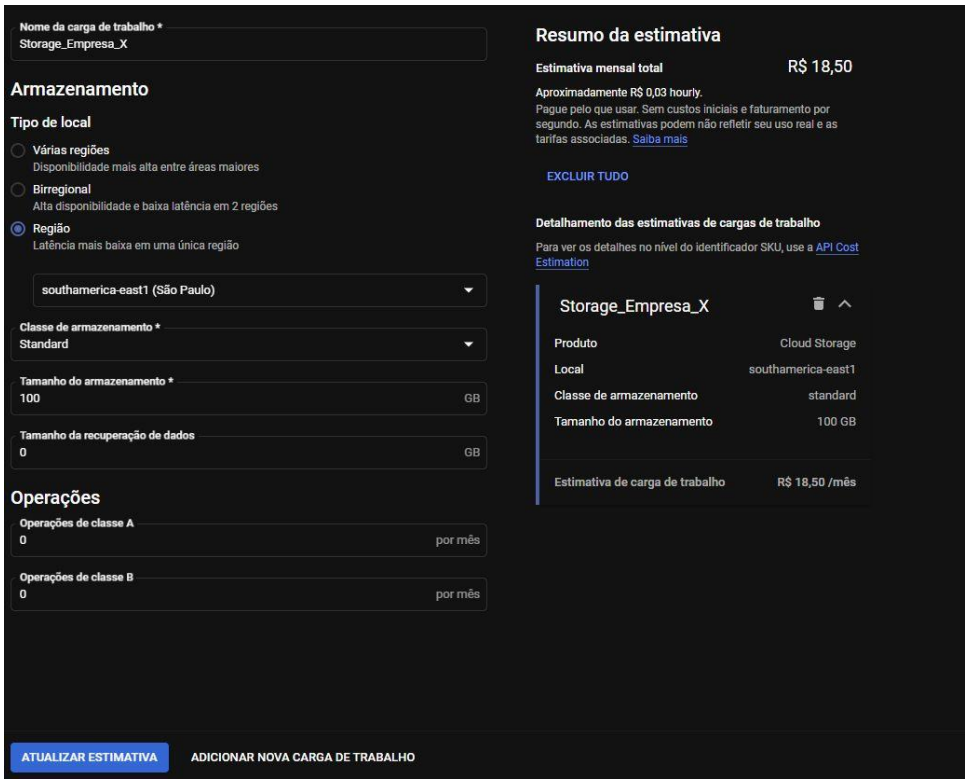
A ferramenta *Veeam Backup and Replication* oferece recursos avançados para facilitar essas rotinas e garantir a proteção dos dados críticos. Neste trabalho, foram definidos os agendamentos de backup para cada máquina virtual, levando em consideração a frequência de alterações nos dados e a janela de backup disponível. Além da execução e configuração de backups incrementais regulares das VMs e recuperação de perda.

Em suma, a implementação de estratégias adequadas de backups como a utilização de sites em diferentes regiões, backups em diferentes camadas e testes regulares são práticas indispensáveis para integridade de ambientes de tecnologia da informação.

Tendo em vista os aspectos mencionados, o cenário aplicado na empresa X apresentada no estudo de caso, apresentou uma solução híbrida envolvendo o *backup* local e um serviço de armazenamento em nuvem, que corroborou na eficiência em escalar e proteger os dados, por conseguinte, fornecendo maior confiabilidade nas tomadas de ações corretivas em caso de falhas, sendo fundamental para eficácia do plano de backup e infraestrutura associada. Futuramente pretende-se verificar a possibilidade de criar uma infraestrutura que faça uso de ferramentas de backup gratuitas com intuito de reduzir custos empresariais.

ANEXO A

Figura A1 – Estimativa da carga de trabalho no Google Cloud Storage



Fonte: Elaborado pelo autor

REFERÊNCIAS

AL-OMARI R.; SOMANI, A. K. G. **Efficient overloading techniques for primary-backup scheduling in real-time systems**. In: [S.l.: s.n.], 2004. v. 64, p. 8629–648.

CONTROLE Net. Disponível em: https://www.controle.net/faq/tipos-de-backup-o-que-e-backup-full-incremental-e-diferencial. Acesso em: 08 de Junho de 2023.

DICIO, **Dicionário Online de Português**. 2023. Disponível em: https://www.dicio.com.br/backup/. Acesso em: 15 de Junho de 2023.

GDSOLUTIONS. **Entenda a importância do backup para empresas**. 2016. Disponível em: https://globaldata.com.br/entenda-a-importancia-do-backup-para-empresas/. Acesso em: 08 de Junho de 2023.

GOMES, N. dos S. **Os Processos de Formação De Neologismos**. Rio de Janeiro: [s.n.], 2015. Disponível em:http://www.filologia.org.br/rph/ANO21/61supl/073.pdf. Acesso em 20 de maio de 2023.

IBM. ***Criptografia***. 2023. Disponível em: https://www.ibm.com/docs/pt-br/ibm-mq/9.2?topic=concepts-cryptography. Acesso em: 30 de Maio de 2023.

MICROSOFT. ***Windows 11***. 2022. Disponível em: https://www.microsoft.com/pt-br/windows/?r=1. Acesso em: 15 de Junho de 2023.

NAIK, D. C. **Backup and Restore - Technologies for Windows**. Disponível em: https:http://www.informit.com/articles/ article.aspx?p=99985, 2003, note = Acesso em: 08 de Junho de 2023.

NETO, C. C.; PINTAS, J. T.; NETO, M. L. V.; SANTOS, M. Gomes de A. **Backup**. *REVISTA DE TRABALHOS ACADÊMICOS-CAMPUS NITERÓI*, 2014. Acesso em: 08 de Junho de 2023. Citado na página 11.

POSTHUMUS S.; VON SOLMS, R. **A framework for the Governance of Information Security**. [S.l.]: Computers Security, v. 23, issue 8, 2004. 638-646 p. Disponível em: https://www.sciencedirect.com/science/article/abs/pii/S0167404804002639. Acesso em 20 de maio de 2023.

ROTARU, O. P. **Além dos Objetivos de Recuperação de Desastres Tradicionais - Aumentando as Características de Consistência de Recuperação**. 2012. 1 p.

SENGUPTA SHUBHASHIS E ANNERVAZ, K. **Distribuição de dados em vários locais para recuperação de desastres - Uma estrutura de planejamento**. [S.l.]: Elsevier, 2014. 53–64 p.

SILVA E. L.,.M. E. M. **Metodologia da pesquisa e elaboração de dissertação**. (4a ed). Florianópolis: UFSC.: [s.n.], 2005. Disponível em: https://tccbiblio.paginas.ufsc.br/files/2010/09/024_Metodologia_de_pesquisa_e_elaboracao_de_teses_e_dissertacoes1.pdf. Acesso em: 14 de Junho de 2023.

SOFTWARE, V. **Veeam Backup and Replication 12**. 2023. Disponível em: https://www.veeam.com/vm-backup-recovery-replication-software.html?ad=menu-products. Acesso em: 15 de Junho de 2023.

SPANIOL, B. **Quatro tipos de Backup**. Disponível em: https://www.aliancatecnologia.com/conteudo/2015/05/quatro-tipos-de-backup/, note = Acesso em: 08 de Junho de 2023.

VEEAM Backup Como Funciona. Disponível em: https://comoaprenderwindows.com.br/ veeam-backup-como-funciona/. Acesso em: 15 de Junho de 2023.