

The logo for ArCloud, featuring the text "ArCloud" in a white, sans-serif font. The letter "A" is stylized with a horizontal bar extending to the left. A small purple square is positioned to the right of the letter "d". The logo is set against a dark blue rectangular background.

ArCloud<sup>®</sup>

CLOUD - Data Protection

# Veeam Service Provider Console

MANUAL DE UTILIZADOR

Referência: M\_GP\_302

Data: 21/05/2026

Versão: 3.0

### Controlo de Versões:

Versão	Data	Alterações
1.0	31-10-2024	na.
2.0	11-02-2026	Nova imagem Ar
3.0	21-05-2026	Atualização para a versão 13 do Veeam

## Significado dos símbolos utilizados



---

INFORMAÇÃO

Informação adicional que se pretende destacar



---

AVISO

Informação Importante que requer especial atenção

---

## ÍNDICE

1. MANUAL DE UTILIZADOR .....	5
2. ACESSO .....	6
3. OPERAÇÃO.....	7
3.1 Gestão de Utilizadores .....	7
3.2 Gestão de Localizações.....	11
3.3 Instalação do agente de gestão .....	12
3.3.1 Instalar o Agente Windows.....	14
3.3.2 Instalar o Agente Linux.....	14
3.3.3 Instalar Agente MAC.....	15
3.3.4 Máquinas encontradas e estado dos agentes .....	16
3.4 Discovery.....	16
3.5 Instalação do agente de backup .....	21
3.6 Remoção de agentes .....	24
3.7 Configurar um backup job .....	27
3.8 Criação/edição de políticas de backup.....	30
3.9 Gestão de backup jobs .....	38
3.10 Recuperação granular de ficheiros via portal .....	40
3.11 Recuperação completa da máquina .....	45
3.11.1 Criação do meio de recuperação em máquinas Windows.....	45
3.11.2 Criação do meio de recuperação em máquinas Linux.....	49
3.11.3 Recuperação com base no Recovery Media Windows .....	49
3.11.4 Recuperação com base no Recovery Media Linux .....	57
3.12 Recuperação de itens aplicativos.....	65

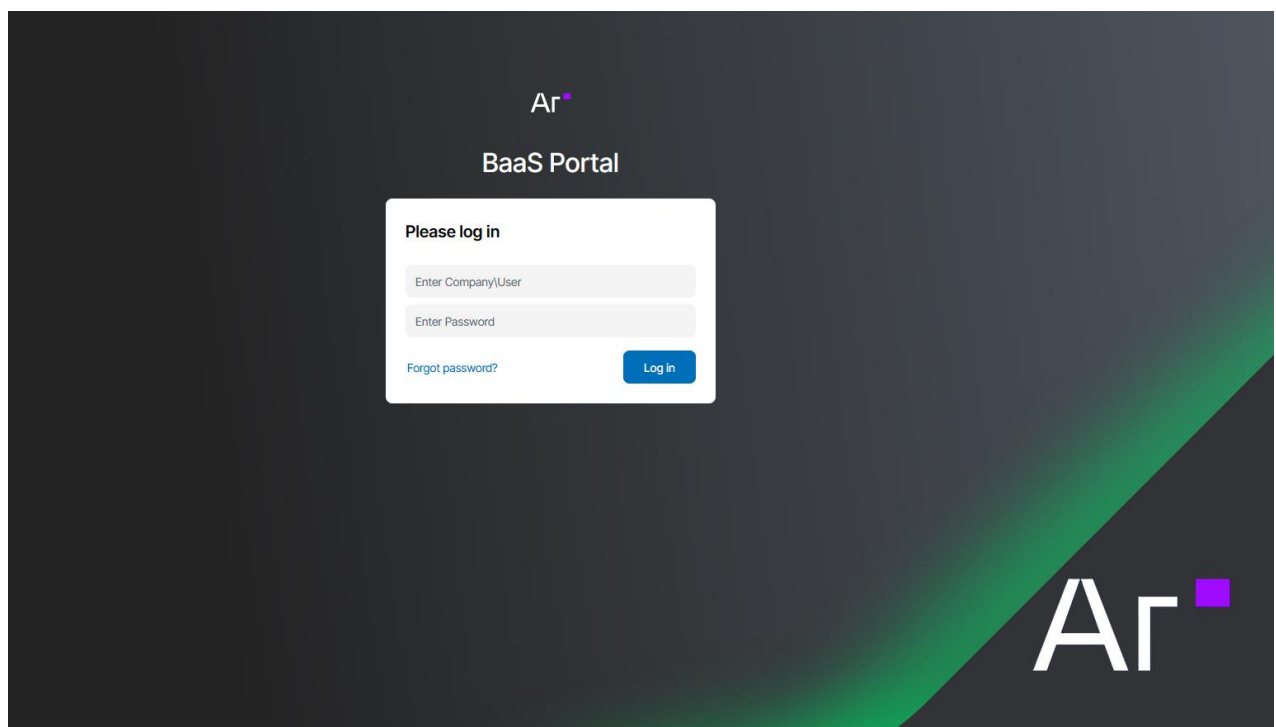
## 1. MANUAL DE UTILIZADOR

Este documento tem como objetivo facilitar a utilização da consola dos serviços de proteção de dados da Ar baseados na tecnologia Veeam e é uma simplificação da documentação da Veeam, adaptada para os cenários mais comuns. Para obter informações e formação mais detalhadas, recomendamos que visite <https://www.veeam.com/pt/products/service-provider/console/resources.html>

## 2. ACESSO

A plataforma de gestão dos serviços **Backup as a Service** e **365 Backup**, está disponível através de endereço URL público, sendo por isso acessível de qualquer parte do mundo através de browser com acesso à internet. Sempre que o cliente contrata um destes serviços, a Ar cria a entidade e um utilizador com os privilégios relevantes, e envia por email a ficha de acesso ao serviço.

Antes de aceder ao portal, deve confirmar os dados disponibilizados pela equipa de provisão da Ar, presentes no e-mail de Boas Vindas, que consistem no nome de utilizador e respetiva Organização, a palavra-chave e o URL de acesso. O acesso à consola faz-se então através de web browser seguindo o seguinte URL: <https://dpconsole.artelecom.pt:1280>



---

É necessário que a comunicação para o exterior da sua organização através da porta TCP 1280 não esteja bloqueada por firewall ou software anti-malware.

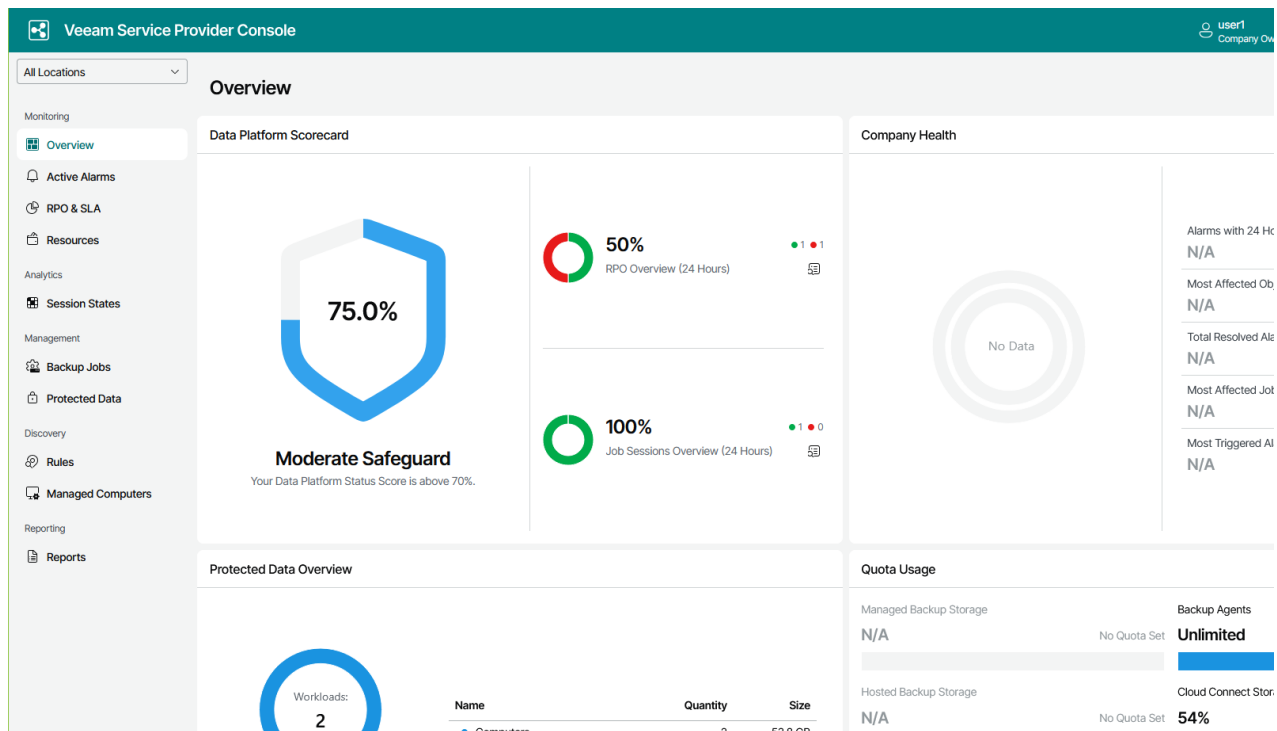
---

Para aceder, introduzir o utilizador e password enviados pela Ar, no formato **Company Name\User**.

Se a Autenticação Multi Factor estiver ativa, será solicitado o código gerado pela aplicação autenticadora. Por defeito, o acesso é entregue em modo de autenticação simples, podendo ser alterada posteriormente pelo cliente.

### 3. OPERAÇÃO

Após o login efetuado, será redirecionado para o “Dashboard” onde pode visualizar inicialmente os alarmes ativos. É aqui que pode verificar o estado da infraestrutura protegida, das tarefas de backup, da quota total e disponível e os relatórios e alertas do sistema.



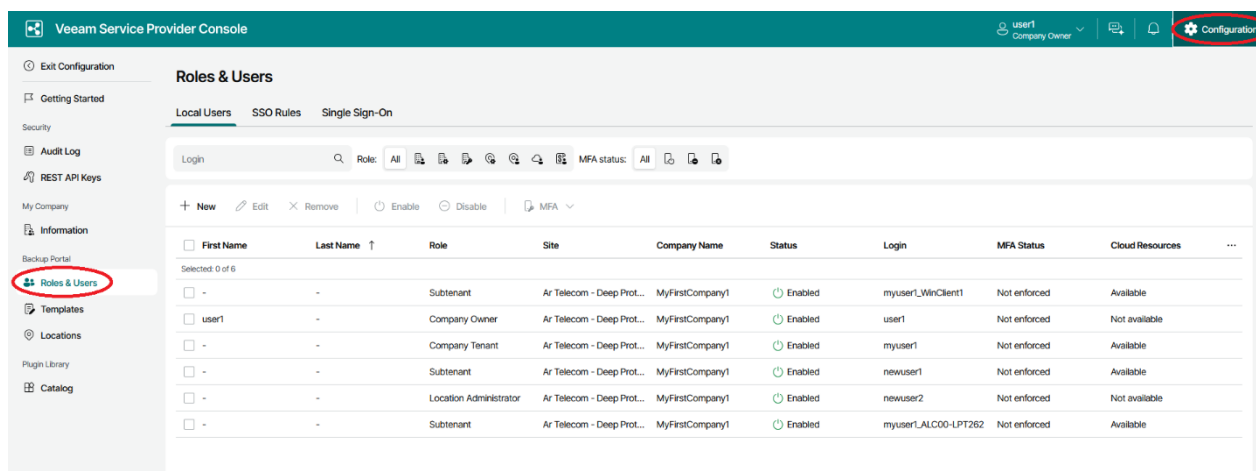
#### 3.1 Gestão de Utilizadores

Com a criação da Companhia é também criado o utilizador “Company Owner” com permissões totais sobre a Companhia. É possível e desejável criar outros utilizadores com perfis distintos, o que pode ser feito inicialmente pelo Company Owner ou posteriormente por utilizadores com perfil Administrator ou Operator.



Não é possível apagar, inibir ou alterar o perfil do utilizador Company Owner.

Para aceder à configuração de utilizadores, carregar em “Configuration” no canto superior direito, seguido de “Roles & Users” no menu lateral esquerdo:



O utilizador de uma companhia pode estar associado a um dos seguintes perfis:

- **Company Owner:** utilizador criado pelo reseller aquando da criação da companhia. Este utilizador não pode ser alterado nem eliminado.
- **Company Administrator:** este utilizador tem as mesmas permissões que o Company Owner mas pode ser eliminado pelo último.
- **Location Administrator:** permite gerir todo o processo de configuração e execução de cópias de segurança e restauros.
- **Location User:** estes utilizadores apenas têm permissão de leitura de informação parcial.
- **Company Invoice Auditor:** este perfil apenas dá acesso ao menu "Invoices" onde pode consultar e processar informação sobre faturação.
- **Subtenant:** Utilizador associado a uma localização e quota de repositório específicos.



Uma vez criado um utilizador de uma companhia, já não é possível modificar o seu perfil.

De seguida apresentam-se as instruções para criar utilizadores locais nas companhias. Também é possível definir configurações **Single Sign-On**, sendo que para isso é necessário primeiro adicionar um **Identity Provider** seguido da criação das regras de SSO. As instruções para tal não se encontram no âmbito deste documento devendo para isso consultar o site da Veeam <https://www.veeam.com/pt/products/service-provider/console/resources.html>

Para criar um utilizador local da Companhia, carregar em "New" no separador "Local Users":

**Roles & Users**

Local Users   SSO Rules   Single Sign-On

Login  Role: All      MFA status: All

**+ New**  Edit  Remove  Enable  Disable  MFA

<input type="checkbox"/>	First Name	Last Name ↑	Role	Site	Company Name	Status	Login	MFA Status
Selected: 0 of 6								
<input type="checkbox"/>	-	-	Subtenant	Ar Telecom - Deep Prot...	MyFirstCompany1	🟢 Enabled	myuser1_WinClient1	Not enforced
<input type="checkbox"/>	user1	-	Company Owner	Ar Telecom - Deep Prot...	MyFirstCompany1	🟢 Enabled	user1	Not enforced
<input type="checkbox"/>	-	-	Company Tenant	Ar Telecom - Deep Prot...	MyFirstCompany1	🟢 Enabled	myuser1	Not enforced
<input type="checkbox"/>	-	-	Subtenant	Ar Telecom - Deep Prot...	MyFirstCompany1	🟢 Enabled	newuser1	Not enforced
<input type="checkbox"/>	-	-	Location Administrator	Ar Telecom - Deep Prot...	MyFirstCompany1	🟢 Enabled	newuser2	Not enforced
<input type="checkbox"/>	-	-	Subtenant	Ar Telecom - Deep Prot...	MyFirstCompany1	🟢 Enabled	myuser1_ALC00-LPT262	Not enforced

O passo seguinte é o de escolher o perfil a atribuir ao utilizador. É possível obter informação mais detalhada sobre as permissões de cada tipo de perfil seguindo o link apresentado neste quadro.

**New User**

- Role**
- User Info
- Login Info
- Multi-Factor Authentication
- Summary

**Role**  
Specify a role to assign to the user.

Role:

**i** Company Administrator has access to all monitoring, reporting, and billing data and can perform all types of management actions. This role cannot modify or remove the Company Owner account.

[Click here to get detailed information on the permissions for each user role.](#)

**New User**

- Role**
- User Info
- Login Info
- Multi-Factor Authentication
- Summary

**Role**  
Specify a role to assign to the user.

Role:

- Company Administrator**
- Location Administrator
- Location User
- Company Invoice Auditor
- Subtenant

**i** Company Administrator has access to all monitoring, reporting, and billing data and can perform all types of management actions. This role cannot modify or remove the Company Owner account.

[Click here to get detailed information on the permissions for each user role.](#)

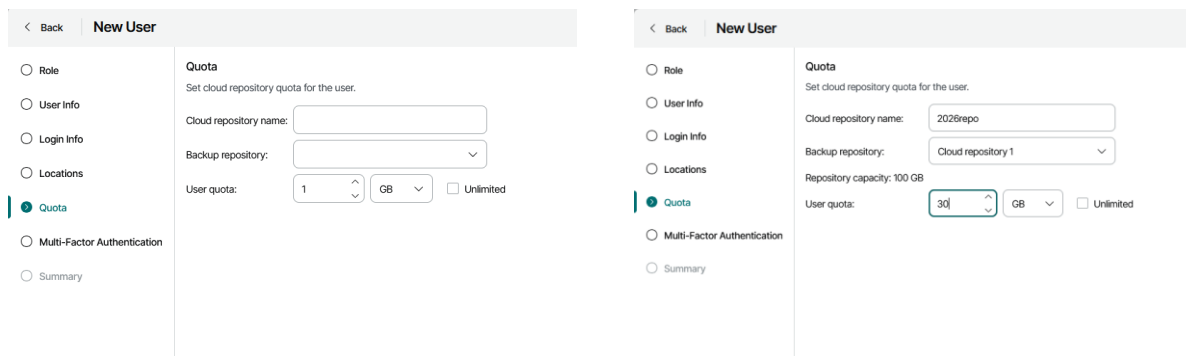
A informação sobre o utilizador é recomendada, embora opcional. Pode ser deixada em branco, bastando preencher a informação de login:

No caso do utilizador a criar ter perfil *Location Administrator*, *Location User* ou *Subtenant* é necessário configurar quais as localizações da companhia a que tem acesso. Assim sendo, é necessário seleccionar as localizações no próximo quadro, carregando na selecção de localizações, seleccionar as pretendidas e carregar "Apply":

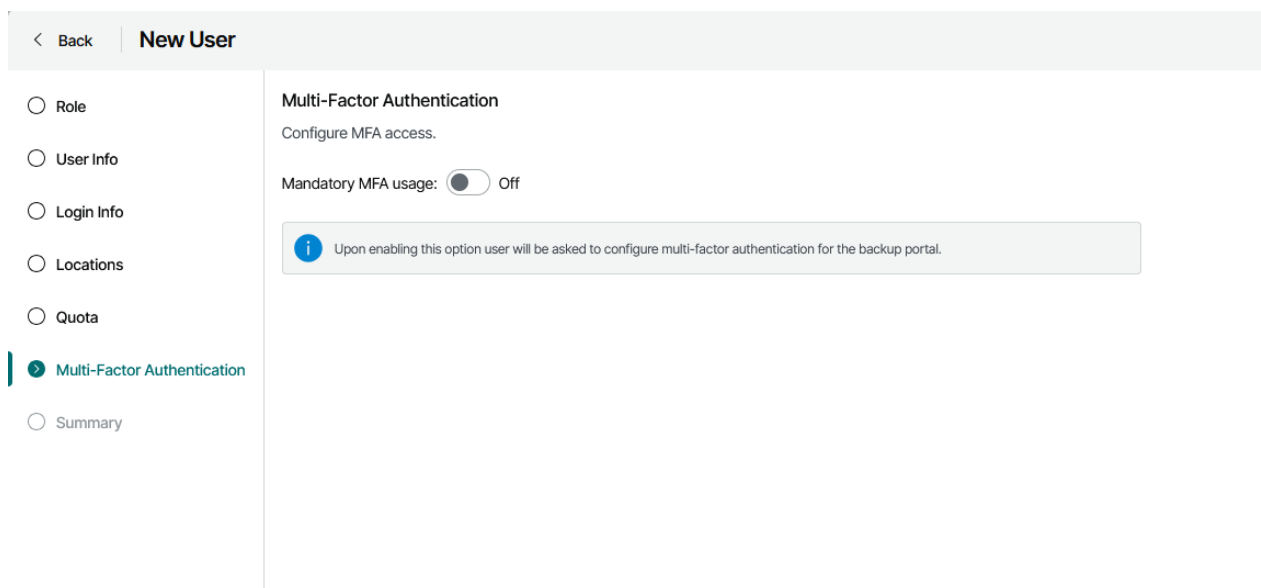
As companhias são criadas sem especificar localizações, pelo que, a única disponível será a "Remote". Depois de configuradas novas localizações, as mesmas estarão disponíveis para selecção neste quadro.

Location	Admins	Users
<input type="checkbox"/> Remote	2	2
<input type="checkbox"/> Site A	2	2

No caso da criação de um utilizador com perfil *Subtenant*, o próximo quadro será para configuração da quota de repositório do mesmo. Assim, é necessário dar um nome ao repositório específico para este utilizador, qual repositório atribuído à companhia e quanto da quota fica disponível para o utilizador. Para isso é necessário ter previamente configurado o repositório atribuído à companhia na secção “*Services*”.



O passo seguinte é o de configurar a obrigatoriedade ou não de autenticação multi-factor.

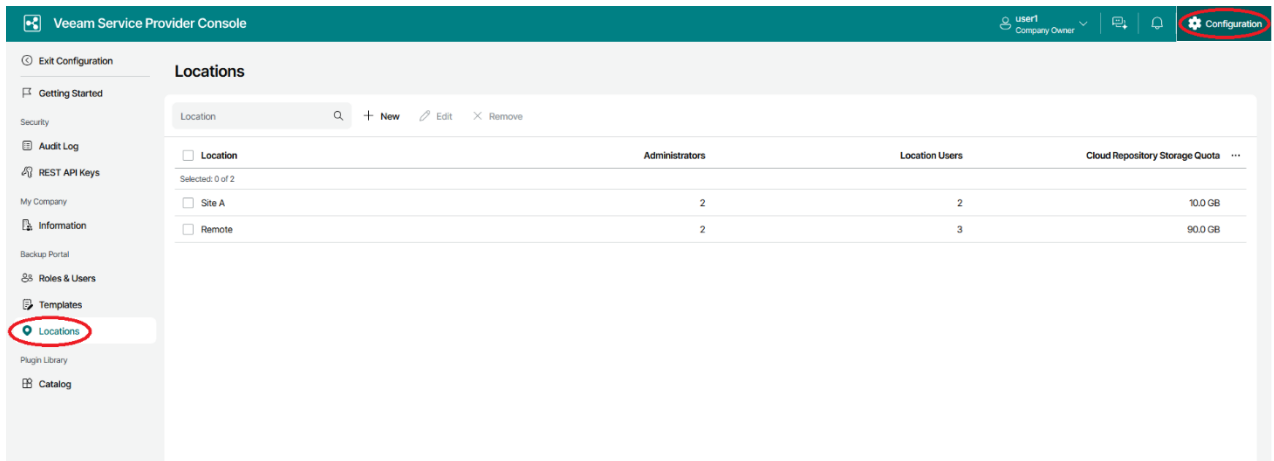


O último passo é rever os dados inseridos e finalizar a criação do utilizador.

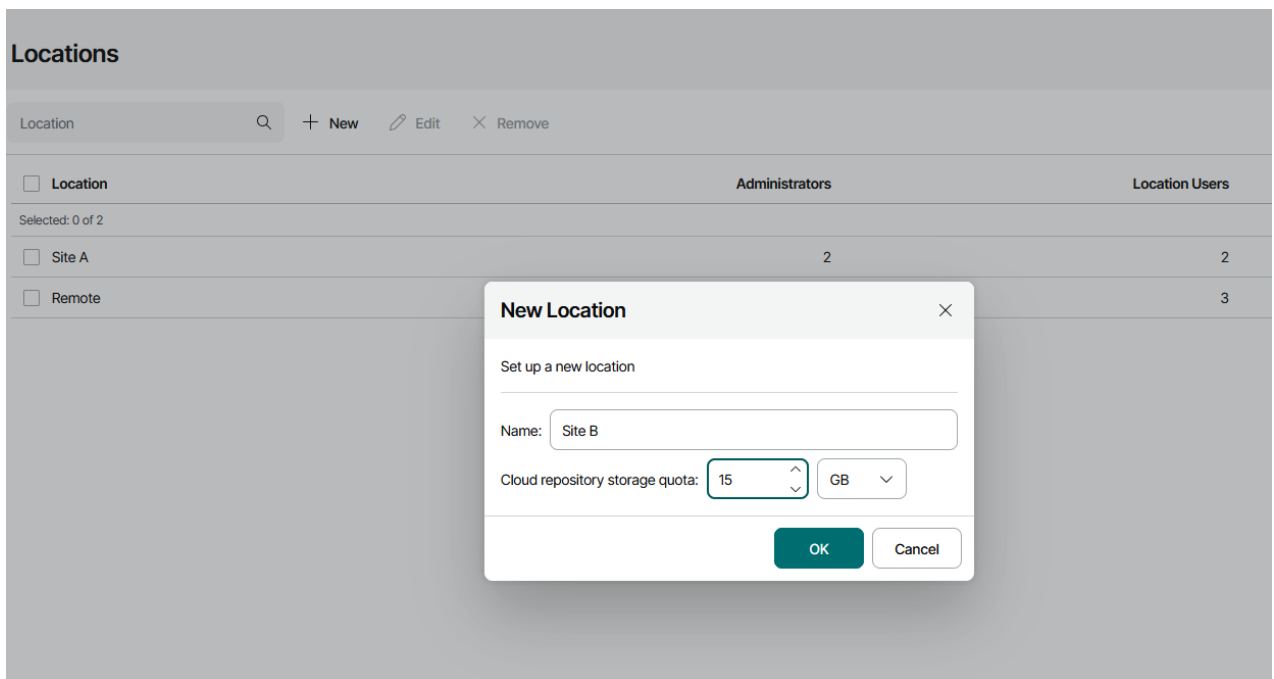
### 3.2 Gestão de Localizações

As companhias podem ter vários locais e querer distinguir recursos por local. Para isso deverão ser configuradas as várias localizações pretendidas. Por defeito, existe uma única localização – “*Remote*”.

As localizações podem ser geridas acedendo a “*Configuration*” na barra superior e escolhendo a opção “*Locations*”:



Aqui pode criar, editar ou remover localizações.



A quota de armazenamento especificada é usada como um limite apenas para informação. Não limita a quantidade real de dados que podem ser carregados para o repositório.

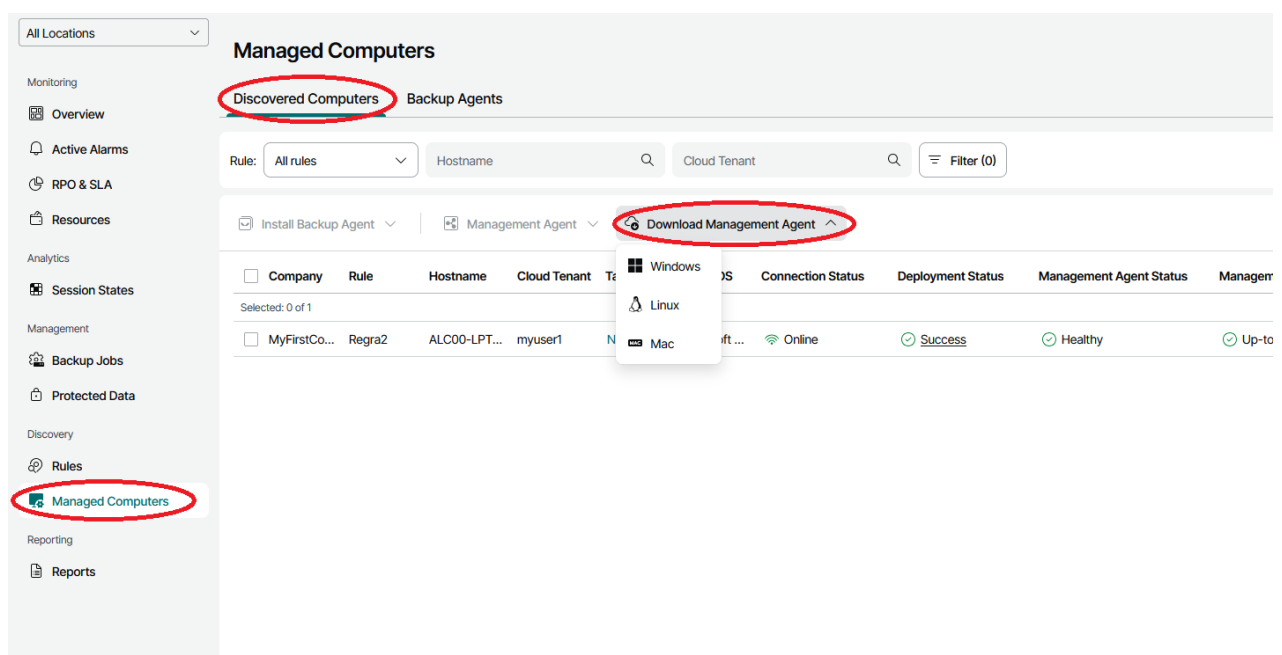
### 3.3 Instalação do agente de gestão

Independentemente dos serviços configurados para a companhia, a consola disponibiliza sempre o "Management Agent" para download.

O agente de gestão permite gerir as máquinas físicas ou virtuais que se ligam à plataforma e facilitar o processo de distribuição dos agentes de backup. É responsável pela atualização dos agentes de backup em todas as máquinas que lhe estão inerentes e permite descobrir máquinas físicas ou virtuais em cada segmento de rede IP da máquina onde estiver instalado.

O agente comunica diretamente com a plataforma da Ar pelo endereço **dpgateway.artelecom.pt** nas portas TCP e UDP 6180, pelo que é necessário que a comunicação através destas portas não esteja bloqueada por firewall ou software anti-malware.

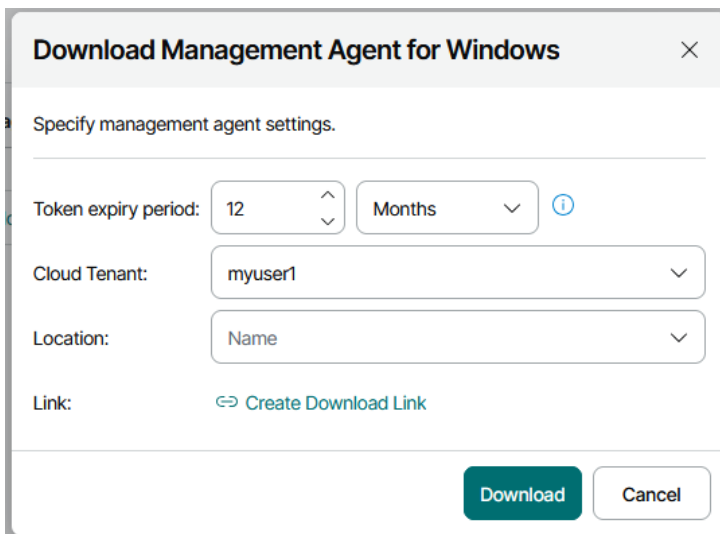
Para obtê-lo ir a "Managed Computers" no menu lateral esquerdo, separador "Discovered Computers" na barra horizontal, seguido de "Download Management Agent", e escolher a plataforma destino pretendida:



The screenshot displays the 'Managed Computers' interface. On the left sidebar, 'Managed Computers' is highlighted. The top navigation bar shows 'Discovered Computers' as the active tab. Below this, there are search filters for 'Rule', 'Hostname', and 'Cloud Tenant'. A dropdown menu for 'Download Management Agent' is open, showing options for 'Windows', 'Linux', and 'Mac'. Below the menu is a table with the following data:

Company	Rule	Hostname	Cloud Tenant	OS	Connection Status	Deployment Status	Management Agent Status	Manager
MyFirstCo...	Regra2	ALC00-LPT...	myuser1	N	Online	Success	Healthy	Up-to

Deve escolher a localização da empresa e a validade do token:

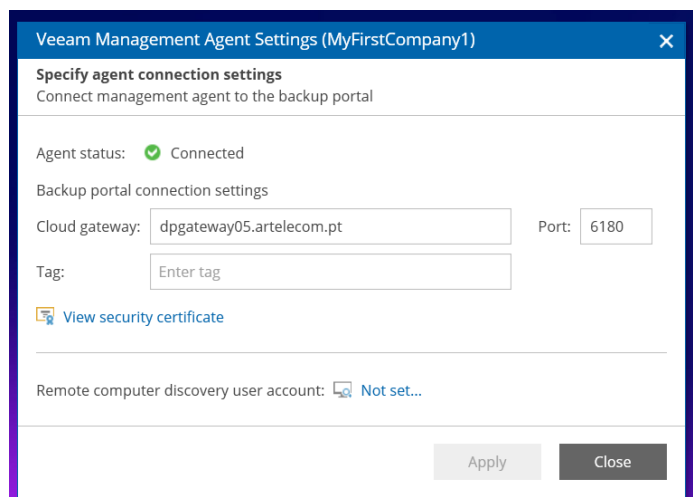
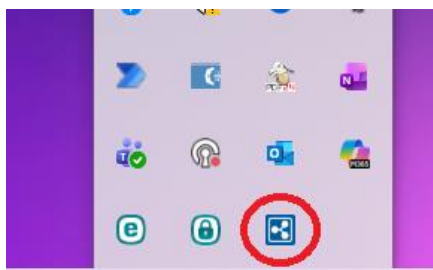


Isto porque o ficheiro a descarregar é específico para a companhia e localização escolhidas. Fim do período de validade do token o instalador deixa de ser válido e é necessário requisitar outro.

### 3.3.1 Instalar o Agente Windows

A instalação do agente do Windows é muito simples, basta aceitar os termos e condições, validar o "License Agreement", aceitar os termos e selecionar "Next".

A partir desse momento, encontra-se visível na barra de tarefas o ícone referente ao "Management Agent". Ao fazer duplo click no mesmo, poderemos ver os detalhes da conexão (podem ser necessários alguns segundos para efetuar a conexão).



### 3.3.2 Instalar o Agente Linux

Primeiro executamos o pacote que descarregámos no Linux, neste caso vamos usar o CentOS.

```
root@LAB1-LNXSRV02:~  
[root@LAB1-LNXSRV02 ~]# ls  
LinuxAgentPackages.mycompany_Default_location.sh  
[root@LAB1-LNXSRV02 ~]# sh LinuxAgentPackages.mycompany_Default_location.sh
```

```
root@LAB1-LNXSRV02:~  
[root@LAB1-LNXSRV02 ~]# ls  
LinuxAgentPackages.mycompany_Default_location.sh  
[root@LAB1-LNXSRV02 ~]# sh LinuxAgentPackages.mycompany_Default_location.sh  
Veeam Management Agent Installation  
Creating temp directory...  
Unpacking installation files...  
Extracting packages...  
System platform: x64  
Installing management agent...  
Installing package veeamma-8.0.0.16877-x64-el7_template.rpm  
Package veeamma-8.0.0.16877-x64-el7_template.rpm installation finished.  
Copying files...  
Configuring agent authentication settings...  
Starting service...  
Configuration summary: Management agent service has been restarted.  
The management agent has been installed.  
Run veeamconsoleconfig -s to get management agent status or veeamconsoleconfig -h to configure the management agent.  
[root@LAB1-LNXSRV02 ~]#
```

Podemos verificar o estado do agente com o comando **veeamconsoleconfig -s**

```
root@LAB1-LNXSRV02:~  
[root@LAB1-LNXSRV02 ~]#  
[root@LAB1-LNXSRV02 ~]#  
[root@LAB1-LNXSRV02 ~]#  
[root@LAB1-LNXSRV02 ~]# veeamconsoleconfig -s  
Management agent  
  Connection state      : Connected  
  Cloud gateway        : dpgateway05.artelecom.pt:6180  
  Connection account    : mycompany  
Backup agent  
  Status                : Not installed  
[root@LAB1-LNXSRV02 ~]#
```

### 3.3.3 Instalar Agente MAC

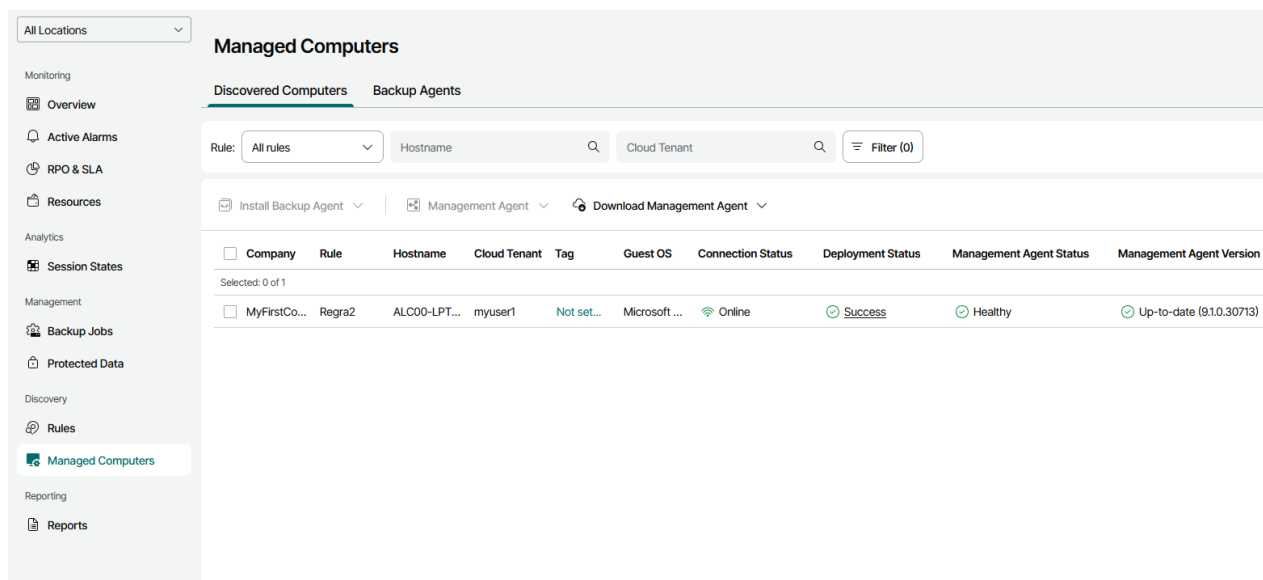
Primeiro executamos o pacote que descarregámos no MAC.

```
iMac-de-AIRE:Downloads aire$ sudo bash MacAgentPackages.sh
Veeam Management Agent Installation
Creating temp directory...
Unpacking installation files...
Installing management agent...
installer: Package name is Veeam Management Agent 5.0.0.6883
installer: Installing at base path /
installer: The install was successful.
Installing backup agent...
OS version: 11.6
Backup agent to install: Veeam Agent for Mac-1.0.0.713.pkg
installer: Package name is Veeam Agent for Mac 1.0.0.713
installer: Installing at base path /
installer: The install was successful.
Installation Complete
Please run veeamconsoleconfig -h to configure the management agent.
```

e verificamos o estado do agente com o comando **veeamconsoleconfig -s**

### 3.3.4 Máquinas encontradas e estado dos agentes

Após a instalação dos agentes de gestão, o quadro "Managed Computers" apresentará as máquinas com agente instalado, assim como as máquinas descobertas segundo as regras que sejam criadas para o efeito.



The screenshot shows the 'Managed Computers' section of the Veeam console. It includes a sidebar with navigation options like 'Monitoring', 'Overview', 'Active Alarms', 'RPO & SLA', 'Resources', 'Analytics', 'Session States', 'Management', 'Backup Jobs', 'Protected Data', 'Discovery', 'Rules', 'Managed Computers', 'Reporting', and 'Reports'. The main area is titled 'Managed Computers' and has tabs for 'Discovered Computers' and 'Backup Agents'. Below the tabs, there are search filters for 'Rule' (set to 'All rules'), 'Hostname', and 'Cloud Tenant', along with a 'Filter (0)' button. There are also buttons for 'Install Backup Agent', 'Management Agent', and 'Download Management Agent'. A table below shows the discovered computers with columns for Company, Rule, Hostname, Cloud Tenant, Tag, Guest OS, Connection Status, Deployment Status, Management Agent Status, and Management Agent Version. One computer is listed: 'MyFirstCo...' with rule 'Regra2', hostname 'ALC00-LPT...', cloud tenant 'myuser1', tag 'Not set...', guest OS 'Microsoft ...', connection status 'Online', deployment status 'Success', management agent status 'Healthy', and management agent version 'Up-to-date (91.0.30713)'. The table indicates 'Selected: 0 of 1'.

## 3.4 Discovery

A instalação do agente de gestão permite que a máquina onde foi instalado seja gerida pela consola do serviço, instalando o agente de backup e executando as políticas de backup definidas e associadas. Além disso, o agente de gestão pode também ser utilizado como veículo para a deteção de outros dispositivos na rede e subsequente instalação de agentes.

Para isso e concluída a instalação e configuração do "Management Agent", procede-se à configuração de uma ou mais regras que serão responsáveis por encontrar servidores e/ou workstations, onde será instalado o agente de backup Veeam. Na página principal, escolher opção "Rules":

All Locations

### Rules

Monitoring

- Overview
- Active Alarms
- RPO & SLA
- Resources

Analytics

- Session States

Management

- Backup Jobs
- Protected Data

Discovery

- Rules**
- Managed Computers

Reporting

- Reports

Rule  Guest OS: All

+ New ^ Edit Remove Run Stop Schedule View Discovered Computers

	Rule	Tenant	Guest OS	Total Computers
<input type="checkbox"/> <input type="checkbox"/> Created	Regra2	myuser1	Windows	1

Escolher o nome para a regra e a que localizações se aplica:

< Back | **New Windows Discovery Rule**

**Rule Name**

Specify the rule name.

Name:

- Rule Name
- Locations
- Discovery Method
- Network Discovery
- Access Account
- Discovery Filters
- Email Notification
- Backup Agent Deployment
- Schedule
- Summary

< Back | **New Windows Discovery Rule**

- Rule Name
- Locations**
- Discovery Method
- Network Discovery
- Access Account
- Discovery Filters
- Email Notification
- Backup Agent Deployment
- Schedule
- Summary

**Locations**  
Select locations accessible for this rule.

Location

<input checked="" type="checkbox"/> Location ↑	Master Agent	Site	Tenant
Selected: 1 of 3			
<input checked="" type="checkbox"/> Remote	ALC00-LPT262	Ar Telecom - Deep Protection	myuser1
<input type="checkbox"/> Site A	No agents installed	-	-
<input type="checkbox"/> Site B	No agents installed	-	-

No próximo passo, apresentam-se os métodos disponíveis para o discovery: baseado em endereçamento IP de rede, via Active Directory ou importação de ficheiro.

< Back | **New Windows Discovery Rule**

- Rule Name
- Locations
- Discovery Method**
- Network Discovery
- Access Account
- Discovery Filters
- Email Notification
- Backup Agent Deployment
- Schedule
- Summary

**Discovery Method**  
Select the desired discovery method.

- Network-based discovery**  
Static discovery defined by the network IP range. Recommended for smaller environments without Active Directory domain.
- Microsoft Active Directory discovery**  
Dynamic discovery defined by Active Directory containers. Recommended for Active Directory domain environments of any size.
- Computers from CSV file**  
Dynamic discovery defined by the content of a comma-separated values (.csv) file with computer names. Recommended for environments which have CMDB integration.

No quadro "Access Account" é necessário inserir credenciais (locais ou de domínio) dos dispositivos onde vai ser instalado o agente de backup Veeam. Estas credenciais necessitam de ter privilégios de administração.

< Back | **New Windows Discovery Rule**

- Rule Name
- Locations
- Discovery Method
- Active Directory Discovery
- Access Account**
- Discovery Filters
- Email Notification
- Backup Agent Deployment
- Schedule
- Summary

**Access Account**  
Specify user credentials with local administrator privileges on the remote computers.

Username:

Password:

Use credentials specified in the master management agent configuration

**i** Note: If master management agent credentials are not set or invalid, discovery rule will use the credentials specified above.

No quadro "Discovery Filters" podem ser definidos vários filtros a aplicar na regra:

< Back | **New Windows Discovery Rule**

- Rule Name
- Locations
- Discovery Method
- Active Directory Discovery
- Access Account
- Discovery Filters**
- Email Notification
- Backup Agent Deployment
- Schedule
- Summary

**Discovery Filters**  
Select filters to apply.

[Edit](#)

Type	Description
By OS type	No filters applied
By application	No filters applied
By platform	No filters applied

É também possível configurar notificações por email para o caso de serem detetados novos dispositivos na regra definida.

< Back | **New Windows Discovery Rule**

- Rule Name
- Locations
- Discovery Method
- Active Directory Discovery
- Access Account
- Discovery Filters
- Email Notification**
- Backup Agent Deployment
- Schedule
- Summary

### Email Notification

Specify email address to send email notifications to.


Send notifications

Once a:  on:  at:

To:

Subject:

Send notification email after the first run

 Email notification will be sent according to the schedule only if new computers are discovered.

A instalação automática dos agentes de backup nos dispositivos encontrados é opcional, podendo a regra apenas identificar novos dispositivos, mas sem efetuar qualquer instalação.

< Back | **New Windows Discovery Rule**


- Rule Name
- Locations
- Discovery Method
- Active Directory Discovery
- Access Account
- Discovery Filters
- Email Notification
- Backup Agent Deployment**
- Schedule
- Summary

### Backup Agent Deployment

Select backup agent installation options.


Discover remote computer without installing backup agent (install backup agent later)

Discover remote computer, install backup agent and assign the selected backup policy

Backup policy to apply:  + Create New... 

Read-only UI access for the backup agent:  On

Set default settings for a Windows backup agent: [Configure...](#)

 Target computers must be part of domain or admin shares must be remotely accessible and "File and Printer Sharing" and "Remote Scheduled Tasks Management (RPC)" rules must be open on the computers firewall.

Finalmente, configura-se a periodicidade de execução da regra ou se apenas é executada a pedido.

[Back](#) | **New Windows Discovery Rule**

- Rule Name
- Locations
- Discovery Method
- Active Directory Discovery
- Access Account
- Discovery Filters
- Email Notification
- Backup Agent Deployment
- Schedule**
- Summary

**Schedule**  
Select scheduling options for the discovery rule.

Run this rule automatically

Daily at: 12:30 AM Everyday Days...

Monthly at: 10:00 AM First Sunday Months...

Periodically every: 1 Hours

Time zone: (UTC+00:00) Dublin, Edinburgh, Lisbon, London

Terminadas as configurações, validam-se os dados introduzidos gravando a regra e permitindo a sua execução imediata.

### 3.5 Instalação do agente de backup

Agora que os dispositivos estão disponíveis na consola, já é possível instalar o agente de backup e atribuir as respetivas políticas. Para isso, selecionar "Managed Computers", separador "Discovered Computers" e de seguida selecionar o servidor ou workstation onde se quer instalar o agente de backup:

All Locations ▼

**Managed Computers**

Discovered Computers Backup Agents

Rule: All rules Hostname Cloud Tenant Filter (0)

Install Backup Agent |  Management Agent Download Management Agent

<input checked="" type="checkbox"/>	Company	Rule	Hostname	Cloud Tenant	Tag	Guest OS	Connection Status	Deployment Status	Management Agent Status	Managemer
Selected: 1 of 1										
<input checked="" type="checkbox"/>	MyFirstCo...	Regra2	ALC00-LPT...	myuser1	Not set...	Microsoft ...	Online	Success	Healthy	Up-to-d

Managed Computers

Ao carregar em "Install Backup Agent" surge uma janela a solicitar uma conta de utilizador com permissões que permitam a instalação do agente, e qual a política de backup a aplicar.



Para que seja possível instalar agentes de backup nas máquinas é necessário que o serviço "Backup agents management" esteja ativo na configuração de serviços.

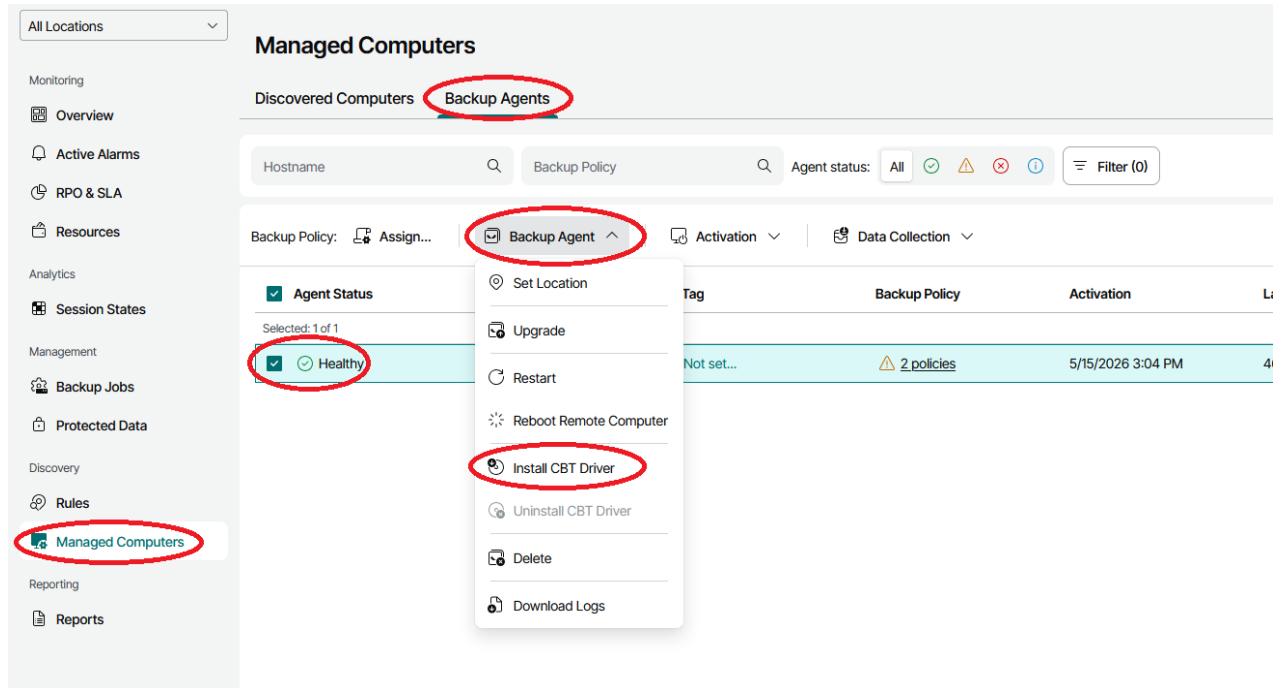
Após fazer *Apply*, pode-se verificar o estado da instalação nas máquinas selecionadas:

Company	Rule	Hostname	Cloud Tenant	Tag	Guest OS	Connection Status	Deployment Status	Management Agent Status
MyFirstCo...	Regra2	ALC00-LPT...	myuser1	Not set...	Microsoft ...	Online	Installing...	Healthy

Carregando em "Installing..." é possível ver o estado da instalação:

Action	Start Time	End Time	Duration
Adding task to the queue	5/15/2026 3:01 PM	5/15/2026 3:01 PM	4 Seconds
Uploading backup agent to the computer	5/15/2026 3:01 PM	5/15/2026 3:01 PM	3 Seconds
Downloading files 1 of 2...	5/15/2026 3:01 PM	5/15/2026 3:01 PM	-
Downloading VeeamAgentWindows.exe...	5/15/2026 3:01 PM	5/15/2026 3:02 PM	47 Seconds
Downloading files 1 of 2...	5/15/2026 3:02 PM	5/15/2026 3:02 PM	-
Downloading VeeamAgentWindows.exe...	5/15/2026 3:02 PM	-	-

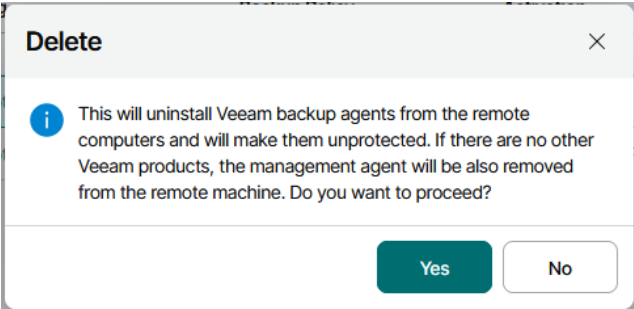
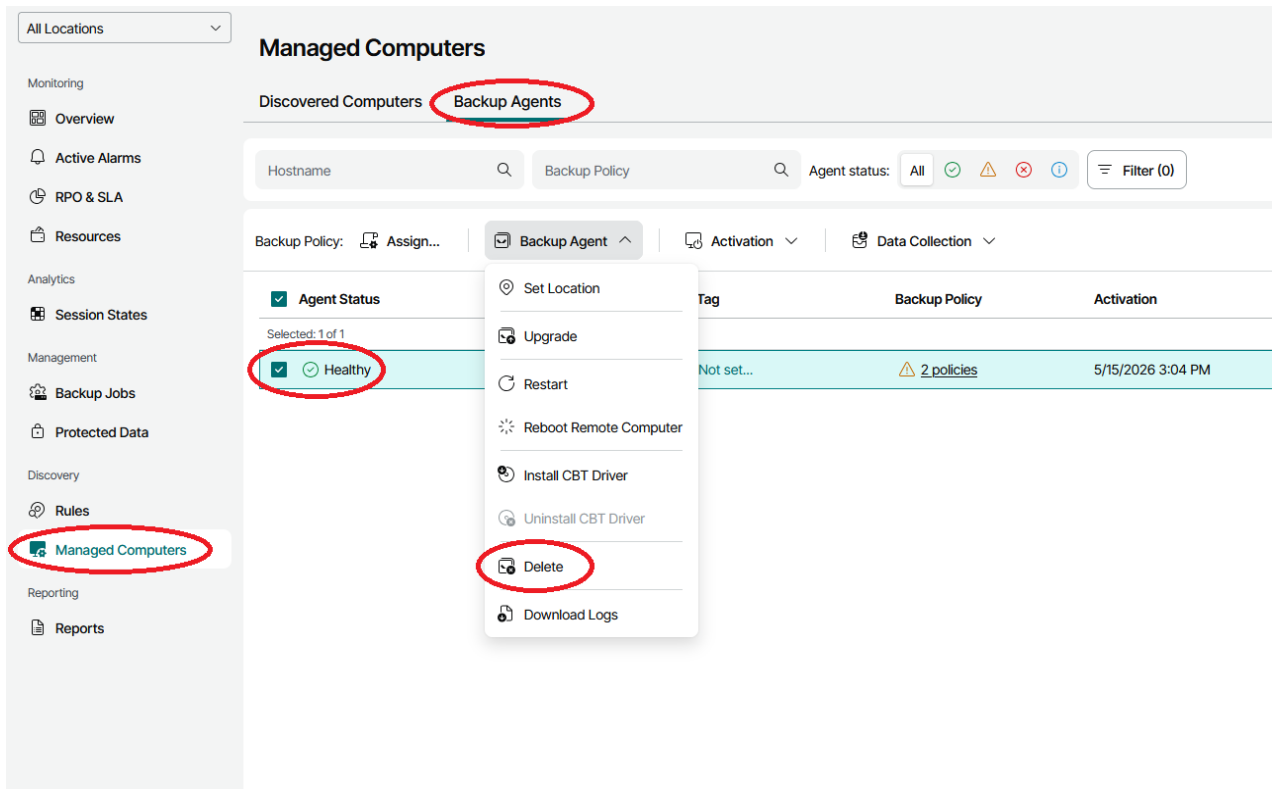
É possível ativar a funcionalidade "CBT Driver" da Veeam (Changed Block Tracking) que facilita o backup incremental. Este driver pode ser instalado com a máquina a funcionar, mas apenas ficará ativo após um reinício da mesma. Para isso, ir a "Managed Computers", separador "Backup Agents", selecionar a máquina pretendida e carregar em "Backup Agent" na barra horizontal depois de selecionar o dispositivo pretendido.



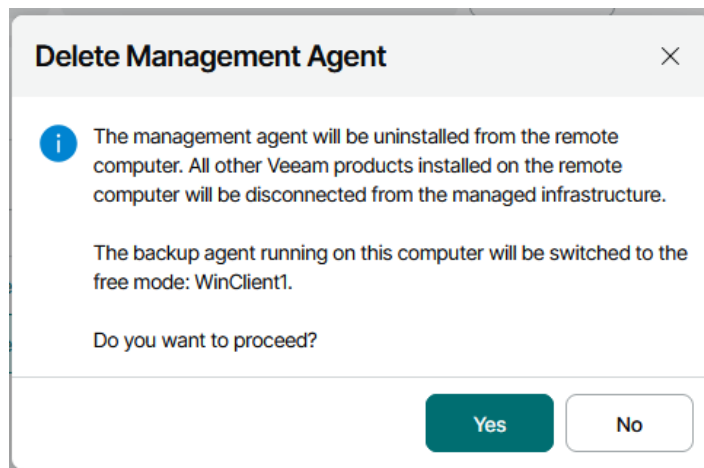
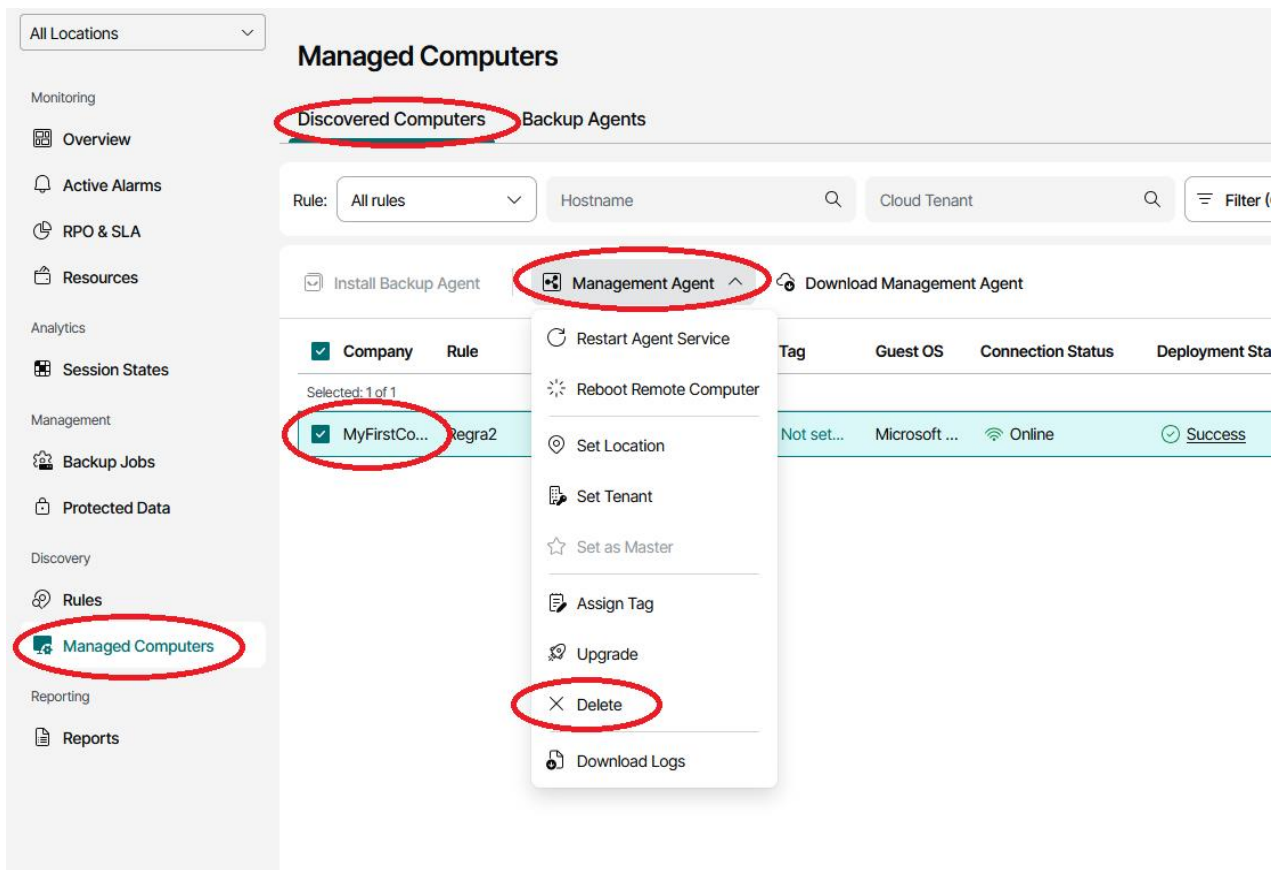
The screenshot shows the Ar Cloud interface for 'Managed Computers'. The 'Backup Agents' tab is selected. A table lists discovered computers with columns for Agent Status, Tag, Backup Policy, and Activation. One agent is selected and its status is 'Healthy'. A context menu is open over this agent, showing options like 'Set Location', 'Upgrade', 'Restart', 'Reboot Remote Computer', 'Install CBT Driver', 'Uninstall CBT Driver', 'Delete', and 'Download Logs'. The 'Install CBT Driver' option is highlighted.

### 3.6 Remoção de agentes

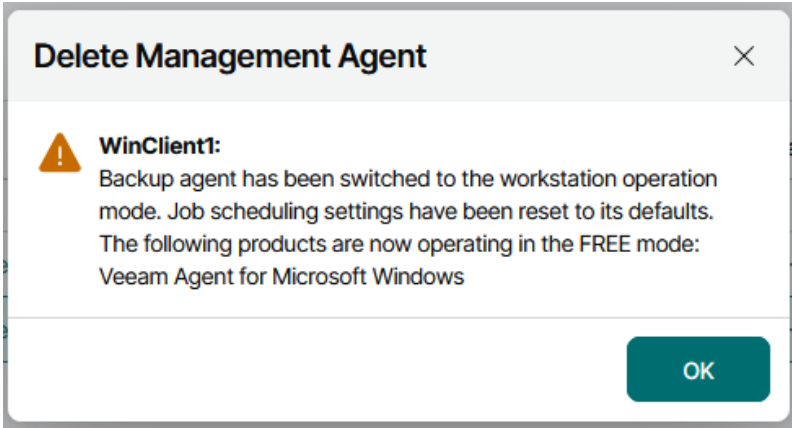
Para remover todos agentes, deve-se remover o agente de backup, escolhendo a máquina de onde se pretende remover:



Ao remover o agente de backup também é removido o agente de gestão.  
Para remover apenas o agente de gestão:

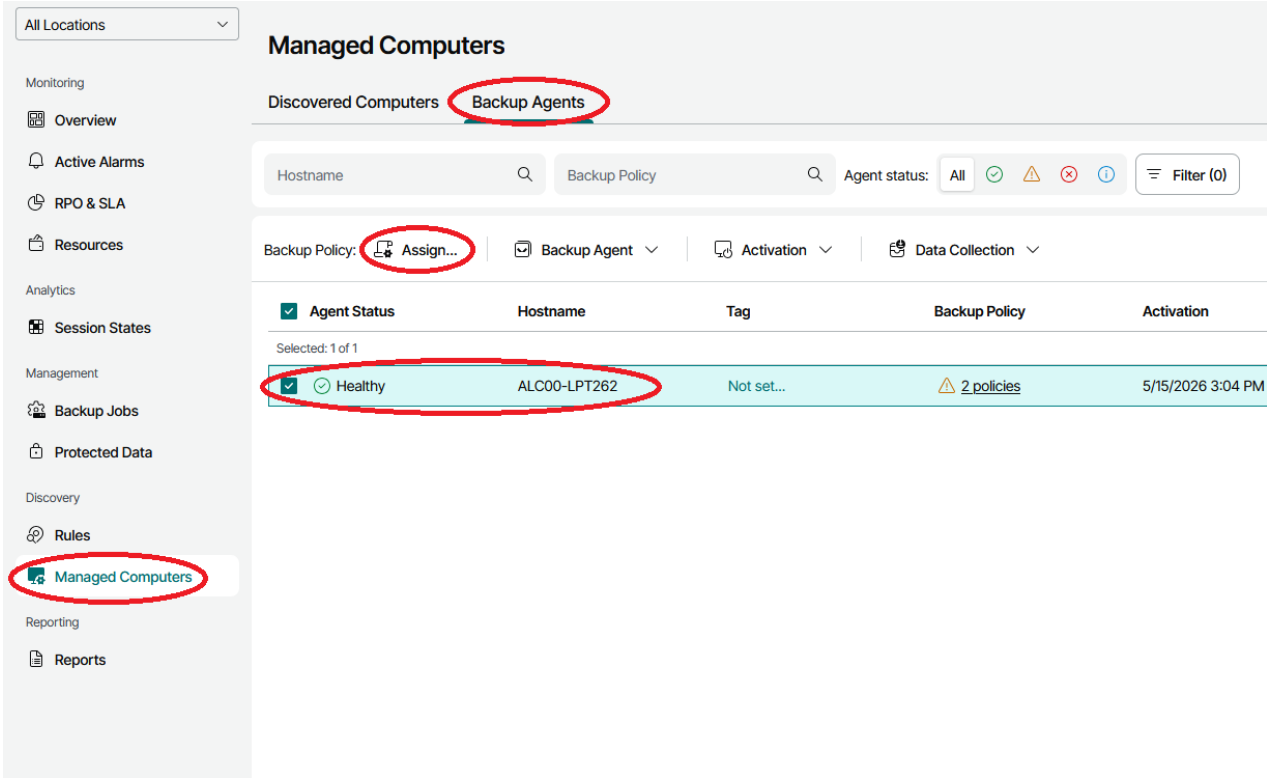


Se o agente de gestão for desinstalado sem desinstalar primeiro o agente de backup, então os agentes de backup geridos por ele ficarão a funcionar em modo "Free", o que quer dizer que deixam de ter acesso ao repositório remoto da Ar. Podem ser usados para efetuar backups e restauros locais. A partir desse momento já não é possível desinstalar o agente de backup via portal.



### 3.7 Configurar um backup job

Agora que o servidor ou a workstation tem o agente de backup instalado, é possível configurar os backup jobs. Para isso, ir a "Managed Computers", tab "Backup Agents", selecionar o servidor ou workstation e assignar uma política, caso não tenha sido selecionado na fase de instalação do agente de backup.



### Backup Policies

Type: All
Guest OS: All

Filter: Guest OS: Windows Clear All

+ Create New Show

<input checked="" type="checkbox"/>	Name	Type	Policy Type	Created by	Description	...
Selected: 1 of 3						
<input checked="" type="checkbox"/>	Workstation: File level b...	Workstation	Created by Provider	Ar Telecom	This policy processes u...	
<input type="checkbox"/>	Server: Entire computer...	Server	Created by Provider	Ar Telecom	This policy should be us...	
<input type="checkbox"/>	MyWkstPolicy2	Workstation	Created by Reseller	LAB_RESELLER	-	

Assign Cancel

Existem já algumas políticas pré-definidas que podem ser usadas, no entanto, é possível criar políticas novas. A partir deste momento a política está aplicada e os backups serão efetuados segundo a mesma.



É possível que surjam avisos sobre diversas situações. Uma situação comum é no caso de não ser possível acordar uma workstation devido aos power settings.

## Discovery

Discovered Computers Backup Agents

Hostname  Backup Policy  Agent status: All ✓ ⚠ ✗ ℹ

Backup Policy: Assign... | Backup Agent | Activation | Data Collection

<input type="checkbox"/> Agent Status	Hostname	Tag	Backup Policy
Selected: 0 of 1			
<input type="checkbox"/> <span>✓</span> Healthy	ALC00-LPT262	Not set...	<span>⚠</span> Warning [Workstation: ...

### Assigned Backup Policies - ALC00-LPT262

Backup Policy  Type: All 📄 🖨

+ Create... ✎ Edit ✕ Delete Job ⚙ Update Config

<input checked="" type="checkbox"/> Name	Type	Description
Selected: 1 of 1		
<input checked="" type="checkbox"/> <span>⚠</span> Warning [Workstation: File		

**Backup Policy** ✕

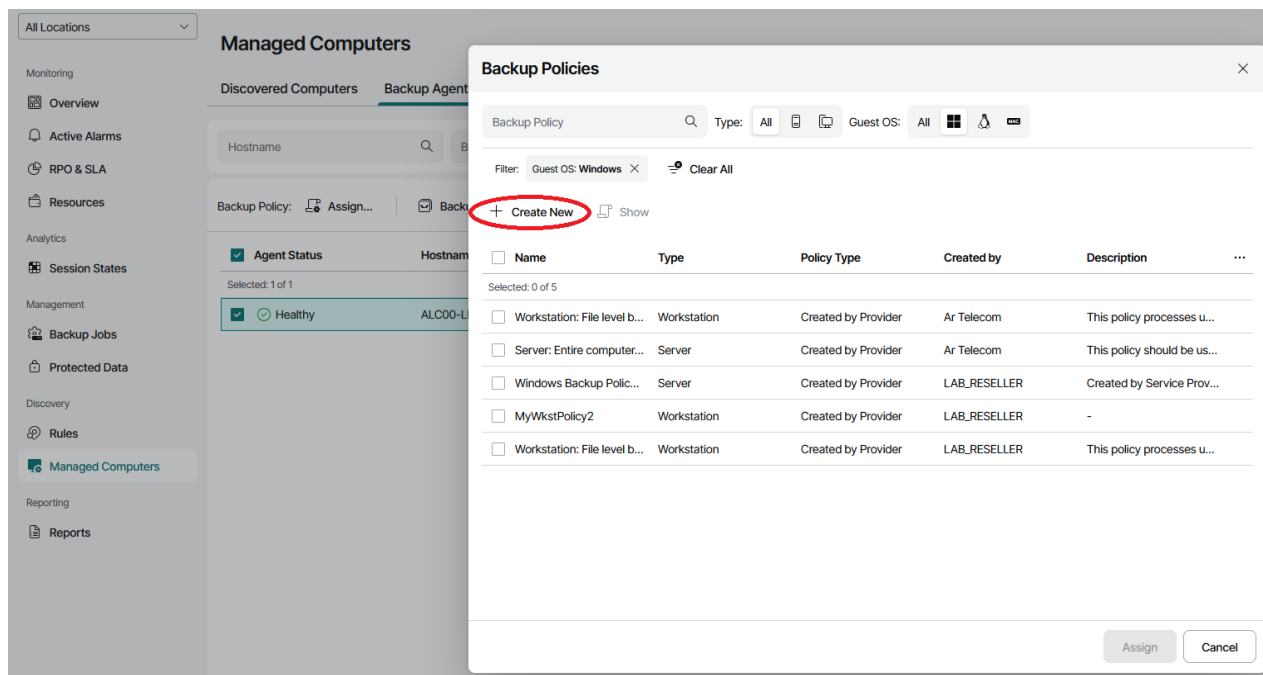
⚠ Backup policy has been applied with a warning.  
 Warning: Wake timers are disabled in the power plan on this computer. Backup agent cannot wake the operating system from sleep to run scheduled backup sessions when such a plan is active. Backup job name: Workstation: File level backup. Personal files. Local drive. Daily schedule.\_ALC00-LPT262.

OK

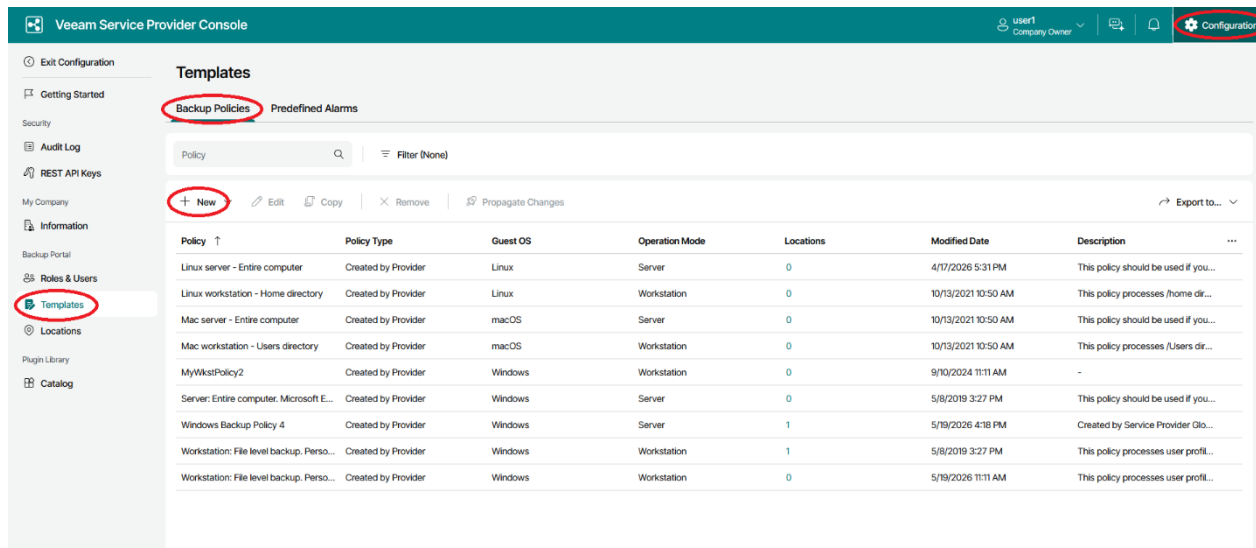
Close

### 3.8 Criação/edição de políticas de backup

A criação ou edição de políticas de backup pode ser feita durante a associação a um agente de backup:

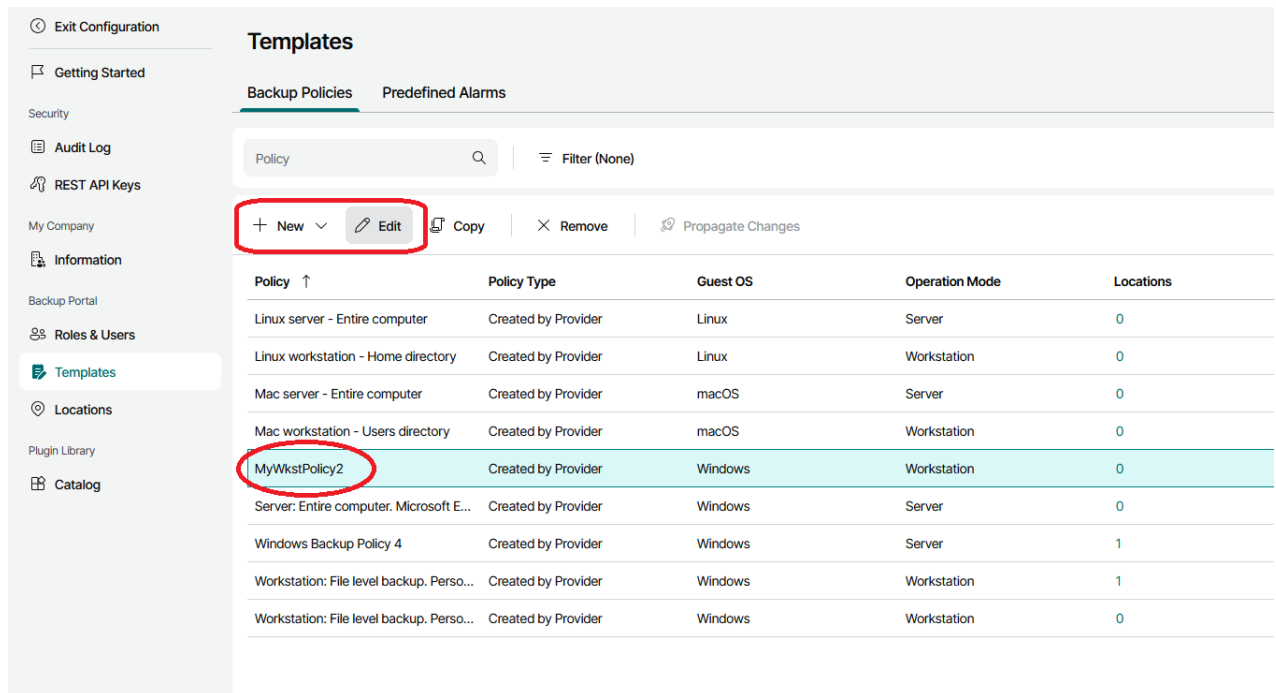


ou indo a "Configuration" no canto superior direito, seguido de "Templates" no menu lateral esquerdo e depois escolhendo a tab "Backup Policies":



Não é possível apagar ou editar as políticas de backup pré-definidas. Pode-se, no entanto, copiar e alterar na nova política criada.

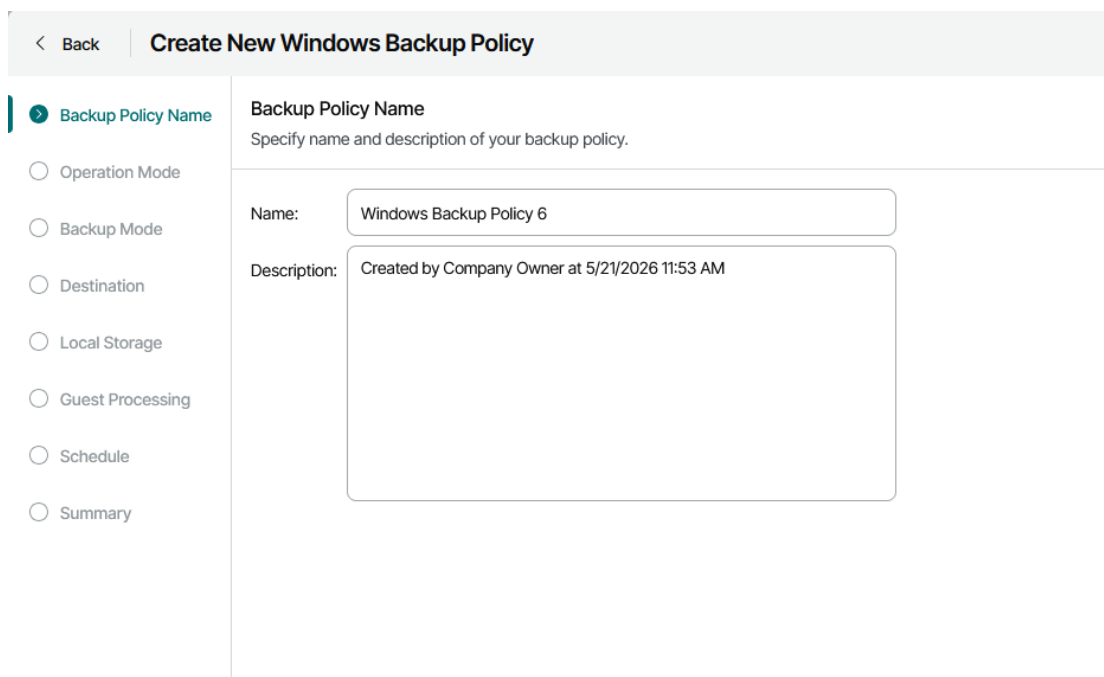
Para editar uma política, seleciona-se a política pretendida e depois carrega-se em "Edit". Para criar, carrega-se em "New":



The screenshot shows the 'Templates' section of the Ar Cloud interface. It features a sidebar on the left with navigation options like 'Exit Configuration', 'Getting Started', 'Security', 'Audit Log', 'REST API Keys', 'My Company', 'Information', 'Backup Portal', 'Roles & Users', 'Templates', 'Locations', 'Plugin Library', and 'Catalog'. The main area is titled 'Templates' and has two tabs: 'Backup Policies' (selected) and 'Predefined Alarms'. Below the tabs is a search bar and a filter dropdown set to 'Filter (None)'. A toolbar contains buttons for '+ New', 'Edit', 'Copy', 'Remove', and 'Propagate Changes'. The '+ New' and 'Edit' buttons are circled in red. Below the toolbar is a table of backup policies:

Policy ↑	Policy Type	Guest OS	Operation Mode	Locations
Linux server - Entire computer	Created by Provider	Linux	Server	0
Linux workstation - Home directory	Created by Provider	Linux	Workstation	0
Mac server - Entire computer	Created by Provider	macOS	Server	0
Mac workstation - Users directory	Created by Provider	macOS	Workstation	0
<b>MyWkstPolicy2</b>	Created by Provider	Windows	Workstation	0
Server: Entire computer, Microsoft E...	Created by Provider	Windows	Server	0
Windows Backup Policy 4	Created by Provider	Windows	Server	1
Workstation: File level backup. Perso...	Created by Provider	Windows	Workstation	1
Workstation: File level backup. Perso...	Created by Provider	Windows	Workstation	0

Ao criar uma política é dado a escolher qual o sistema operativo a que se destina: Windows, Linux ou Mac. O primeiro passo é dar um nome à política a criar:



The screenshot shows the 'Create New Windows Backup Policy' form. It has a 'Back' button and a title 'Create New Windows Backup Policy'. On the left, there is a vertical list of radio buttons for different policy types: 'Backup Policy Name' (selected), 'Operation Mode', 'Backup Mode', 'Destination', 'Local Storage', 'Guest Processing', 'Schedule', and 'Summary'. The main form area is titled 'Backup Policy Name' and includes the instruction 'Specify name and description of your backup policy.' Below this are two input fields: 'Name' with the value 'Windows Backup Policy 6' and 'Description' with the value 'Created by Company Owner at 5/21/2026 11:53 AM'.

De seguida escolhe-se se a política vai ser aplicada a servidores ou workstations. No caso de servidores, existe uma opção mais à frente denominada "Guest Processing" que não existe na versão para workstation.

< Back | Create New Windows Backup Policy

- Backup Policy Name
- Operation Mode
- Backup Mode
- Destination
- Local Storage
- Guest Processing
- Schedule
- Summary

**Operation Mode**  
Select operation mode for the managed backup agent.

- Server**  
Ideal for application server backup due to application-aware backups, guest indexing support and flexible job schedule
- Workstation**  
Designed specifically for end user's computers, laptops and office desktops. Ease of use and friendly job scheduling options

O modo de backup define que tipo de backup se pretende fazer:

- **Entire computer:** cria uma imagem da máquina e permite recuperar em qualquer modo – completo, aplicacional ou granular;
- **Volume level backup:** faz backup apenas dos volumes seleccionados;
- **File level backup:** backup de pastas e ficheiros.

< Back | Create New Windows Backup Policy

- Backup Policy Name
- Operation Mode
- Backup Mode
- Destination
- Local Storage
- Guest Processing
- Schedule
- Summary

**Backup Mode**  
Choose what data do you want to back up from this computer.

- Entire computer (recommended)**  
Back up your entire computer image for fast recovery on any level. Deleted, temporary and page files are automatically excluded from the image to reduce the backup size.  
 Include periodically connected USB drives
- Volume level backup**  
Back up images of selected volumes, for example only data volumes. Deleted, temporary and page files are automatically excluded from the image to reduce the backup size.
- File level backup (slower)**  
Back up individual files and folders by mask. This mode produces an image-based backup with only selected files included in the image.

Caso opte pelo "Volume level backup" surge mais um quadro ("Volumes") com a opção de escolher quais os volumes pretendidos:

< Back | **Create New Windows Backup Policy**

- Backup Policy Name
- Operation Mode
- Backup Mode
- Volumes**
- Destination
- Local Storage
- Guest Processing
- Schedule
- Summary

**Volumes**  
Objects to backup.

Back up selected volumes only  
 Operating system  
Type in the name of the volume you want to backup in the following format "C:\":

C:\ + Add

Remove

Back up all volumes except  
Type in the name of the volume you want to exclude from backup in the following format "C:\":

C:\ + Add

Remove

Caso opte pelo "File level backup" surge mais um quadro ("Files") com a opção de escolher quais as pastas e ficheiros pretendidos:

< Back | **Create New Windows Backup Policy**

Backup Policy Name  
 Operation Mode  
 Backup Mode  
 **Files**  
 Destination  
 Local Storage  
 Guest Processing  
 Schedule  
 Summary

**Files**

Specify objects you would like to include in the backup.

---

**Include files or folders:**  
Specify extension masks or directory paths to include in the backup.  
Directory paths must be specified in the following format: "C:\FolderName". To back up specific files from the directory, set file mask in the following format: "\*.doc"

C:\Program Files + Add

× Remove

Operating system  
 Personal files (8 items of 9)

---

**Exclude files or folders:**  
Specify extension masks to exclude from the backup.  
Use \* to exclude any number of characters, and ? to exclude a single character.  
For excludes, you can additionally specify path to a folder.

\*.jpeg + Add

× Remove

O próximo passo é escolher qual o destino dos backups, existindo quatro opções:

- **Local storage:** faz backup para uma unidade de armazenamento conectada diretamente à máquina a que se está a fazer backup;
- **Shared folder:** faz backup para uma unidade de rede;
- **Veeam backup repository:** faz backup para um repositório gerido por um servidor Veeam Backup & Replication;
- **Veeam Cloud Connect repository:** Esta é a opção a escolher para salvaguardar os backups no repositório fornecido pela Ar.

< Back | **Create New Windows Backup Policy**

- Backup Policy Name
- Operation Mode
- Backup Mode
- Destination**
- Cloud Repository
- Backup Quota
- Backup Cache
- Guest Processing
- Schedule
- Summary

**Destination**  
Choose where you want to back up your data to. We highly recommend that you do not store your backups on the same computer that you are protecting.

- Local storage  
Choose this option to back up to a locally attached storage device such as USB, Firewire or eSATA external hard drive. Backing up to internal hard drives is not recommended.
- Shared folder  
Choose this option to back up to an SMB (CIFS) share on a Network Attached Storage (NAS) device, or on a regular file server.
- Veeam backup repository  
Choose this option to back up to a backup repository managed by Veeam Backup & Replication 12.1 or later server.
- Veeam Cloud Connect repository  
Choose this option to back up to a cloud repository managed by Veeam Cloud Connect server.

Ao configurar o repositório, configura-se também a política de retenção e configurações avançadas. Por defeito, os backups terão uma retenção de 7 dias. É possível escolher a retenção baseada em dias ou pontos de restauro, podendo variar entre 1 e 730 dias ou pontos de restauro.

< Back | **Create New Windows Backup Policy**

- Backup Policy Name
- Operation Mode
- Backup Mode
- Destination
- Cloud Repository**
- Backup Quota
- Backup Cache
- Guest Processing
- Schedule
- Summary

**Cloud Repository**  
The following is the backup retention policy settings for your cloud backups.

Retention policy:  days (excluding days with no backup)

Keep some periodic full backups longer for archival purposes [Configure...](#)

[Advanced settings...](#)

**i** The default cloud repository will be selected from the list of available repositories.

Nas configurações avançadas é possível configurar para efetuar Full Backups:

**Advanced settings** ✕

Backup    Storage-level Corruption Guard    Full Backup File Maintenance    Storage

---

**Synthetic full backups scheduling**

Create synthetic full backups periodically

⚠ This setting will not be applied if backup is targeted to an object storage repository.

Monthly on: First Sunday January, February,...

Weekly on selected days: Sunday

---

**Active full backup**

Create active full backups periodically ⓘ

Monthly on: First Sunday January, February,...

Weekly on selected days: Saturday

No caso de "Veeam Cloud Connect repository", além da configuração da política de retenção e configurações avançadas, é necessário indicar também qual o método de gestão de quota.

< Back | **Create New Windows Backup Policy**

- Backup Policy Name
- Operation Mode
- Backup Mode
- Destination
- Cloud Repository
- Backup Quota
- Backup Cache
- Guest Processing
- Schedule
- Summary

**Backup Quota**  
Set connection account to the cloud repository and define user quota.

---

Use sub-tenant accounts for each managed backup agent with the following quota:

User quota: 100 GB  Unlimited quota

Use single tenant account for all computers managed by the company (not recommended)

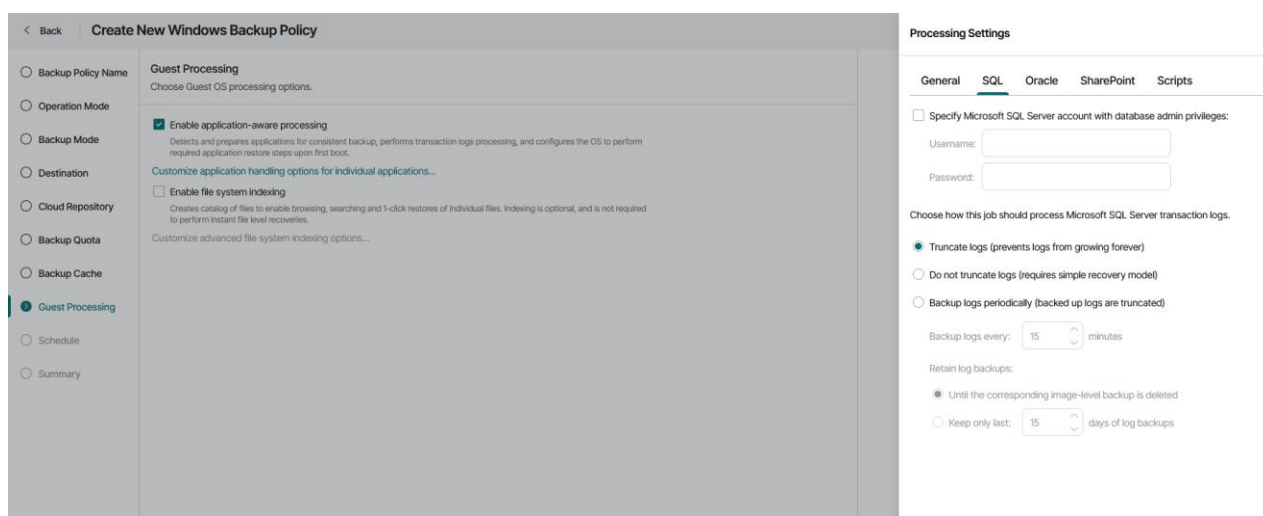
A cache de backup é utilizada no caso de não haver conectividade com o repositório. Nesse caso, é utilizada uma área local com determinado tamanho como destino inicial do backup, sendo que, será transferida para o repositório final assim que a conectividade for restabelecida.

No caso do modo de operação Servidor, é necessário configurar o "Guest Processing". Aqui é possível configurar:

- Processamento application-aware
- Indexação de file system

No processamento de aplicações configuram-se as credenciais de acesso ao MSSQL, Oracle e Sharepoint e se são processados os Transaction Logs.

É também possível configurar a execução de scripts, antes e depois do backup.



The screenshot displays the 'Create New Windows Backup Policy' configuration window. The left sidebar lists various settings: Backup Policy Name, Operation Mode, Backup Mode, Destination, Cloud Repository, Backup Quota, Backup Cache, Guest Processing (selected), Schedule, and Summary. The main area is titled 'Guest Processing' and contains the following options:

- Enable application-aware processing: Detects and prepares applications for consistent backup, performs transaction logs processing, and configures the OS to perform required application restore steps upon first boot.
- Enable file system indexing: Customizes application handling options for individual applications...
- Enable file system indexing: Creates catalog of files to enable browsing, searching and 1-click restores of individual files. Indexing is optional, and is not required to perform instant file level recoveries.
- Customize advanced file system indexing options...

On the right, the 'Processing Settings' panel is shown with tabs for General, SQL (selected), Oracle, SharePoint, and Scripts. Under the 'SQL' tab, there are options for specifying a Microsoft SQL Server account and truncating logs. The 'Truncate logs' option is selected, and the 'Backup logs every' is set to 15 minutes. The 'Retain log backups' section shows 'Until the corresponding image-level backup is deleted' is selected, with 'Keep only last' set to 15 days of log backups.

No último passo configura-se o agendamento dos backups.

[Back](#) | **Create New Windows Backup Policy**

- Backup Policy Name
- Operation Mode
- Backup Mode
- Destination
- Cloud Repository
- Backup Quota
- Backup Cache
- Guest Processing
- Schedule**
- Summary

**Schedule**  
Choose when you want backup job to be started automatically.

Run the job automatically

Daily at this time: 12:30 AM Everyday Monday, Tuesday, ...

Monthly at this time: 10:00 AM First Sunday January, February, ...

Periodically every: 1 Hours Schedule...

Automatic retry

Retry failed job: 3 times

Wait before each retry for: 10 minutes

Terminate job if it exceeds allowed backup window Window...

If the job does not complete within allocated backup window, it will be terminated to prevent snapshot commit during production hours.

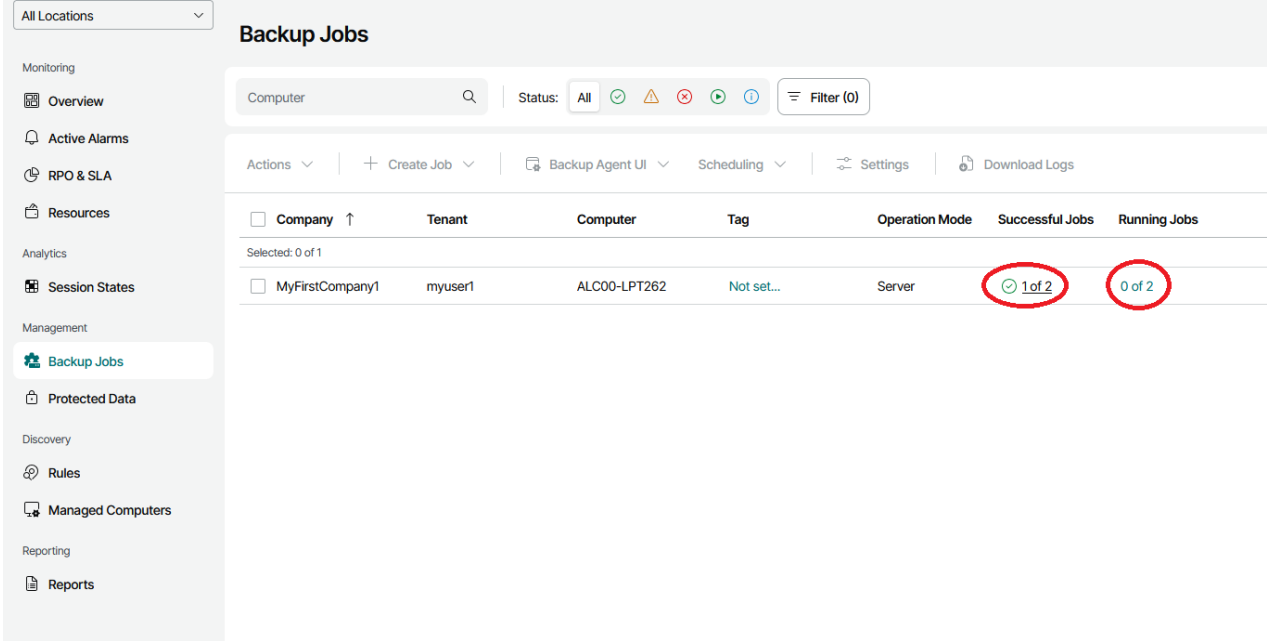
E finalmente revê-se e finaliza-se a configuração.

### 3.9 Gestão de backup jobs

Para visualizar e gerir os backup jobs existentes deve-se carregar em "Backup Jobs" no menu lateral esquerdo:

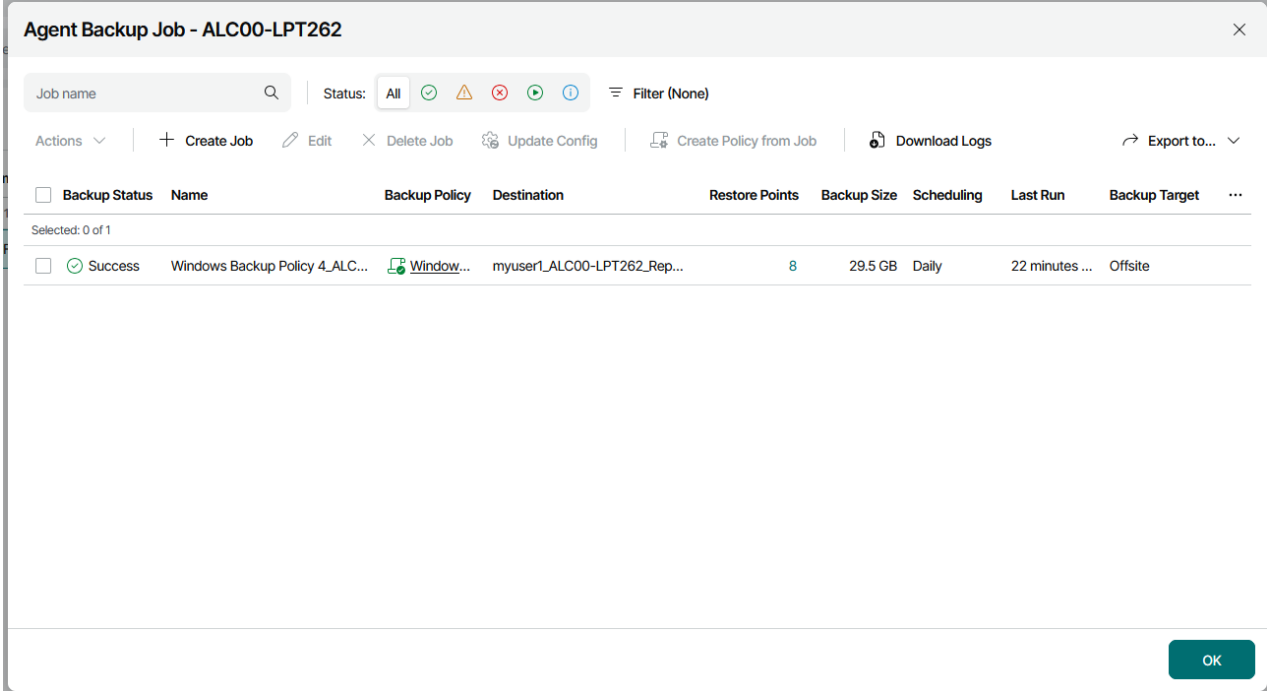
Aqui podemos verificar que jobs e políticas estão configurados, qual o seu estado e quais os executados.

A coluna "Running Jobs" indica para cada máquina, quantos jobs estão configurados e se estão a correr. A coluna "Successful Jobs" indica se foram executados e se foram bem-sucedidos.



Company	Tenant	Computer	Tag	Operation Mode	Successful Jobs	Running Jobs
MyFirstCompany1	myuser1	ALC00-LPT262	Not set...	Server	1 of 2	0 of 2

Carregando sobre os mesmos, quer seja na coluna "Running Jobs" ou "Successful Jobs", obtém-se o detalhe e pode-se fazer várias ações sobre o mesmo:



Backup Status	Name	Backup Policy	Destination	Restore Points	Backup Size	Scheduling	Last Run	Backup Target
Success	Windows Backup Policy 4_ALC...	Window...	myuser1_ALC00-LPT262_Rep...	8	29.5 GB	Daily	22 minutes ...	Offsite

Aqui pode-se:

- Iniciar ou parar a tarefa de execução do backup
- Criar, editar ou apagar uma tarefa de backup
- Aceder aos pontos de restauro

Carregando sobre os pontos de restauro podemos ver uma lista com os vários backups efetuados:

**Agent Backup Job - ALC00-LPT262**

Job name: [Search] | Status: All [Icons] | Filter (None)

Actions: [Create Job] [Edit] [Delete Job] [Update Config] [Create Policy from Job] [Download Logs] [Export to...]

Backup Status	Name	Backup Policy	Destination	Restore Points	Backup Size	Scheduling	Last Run	Backup Target	...
<input type="checkbox"/>	Success	Windows Backup Policy 4_ALC...	Window...	myuser1_ALC00-LPT262_Rep...	8	29.5 GB	Daily	24 minutes ...	Offsite

**Restore Points - Windows Backup Policy 4**

[Export to...]

Backed Up Items	Date ↓	Source Size	Backed Up Data	Restore Point Size
Personal Files	5/19/2026 3:29 PM	-	14.0 GB	1.7 MB
Personal Files	5/19/2026 3:15 PM	-	14.0 GB	1.7 MB
Personal Files	5/19/2026 2:49 PM	-	17.1 GB	1.8 MB
Personal Files	5/19/2026 1:00 PM	-	14.1 GB	3.3 MB
Personal Files	5/19/2026 11:58 AM	-	14.4 GB	1.8 MB
Personal Files	5/19/2026 11:26 AM	-	14.4 GB	14.7 MB
Personal Files	5/19/2026 10:45 AM	-	17.7 GB	15.1 MB
Personal Files	5/18/2026 1:00 PM	-	30.2 GB	29.5 GB

[Close]

### 3.10 Recuperação granular de ficheiros via portal

Para aceder aos backups existentes e respetivos pontos de restauro deve-se ir a "Protected Data" no menu lateral esquerdo:

All Locations

### Overview

Monitoring

- Overview
- Active Alarms
- RPO & SLA
- Resources

Analytics

- Session States

Management

- Backup Jobs
- Protected Data**

Discovery

- Rules
- Managed Computers

Reporting

- Reports

#### Data Platform Scorecard

**75.0%**

**Moderate Safeguard**

Your Data Platform Status Score is above 70%.

**50%**  
RPO Overview (24 Hours)

**100%**  
Job Sessions Overview (24 Hours)

#### Company Health

No

#### Protected Data Overview

#### Quota Usage

Managed Backup Storage  
N/A

Para efetuar um restauro, deve-se selecionar a máquina pretendida e em seguida "File-Level Restore":

All Locations

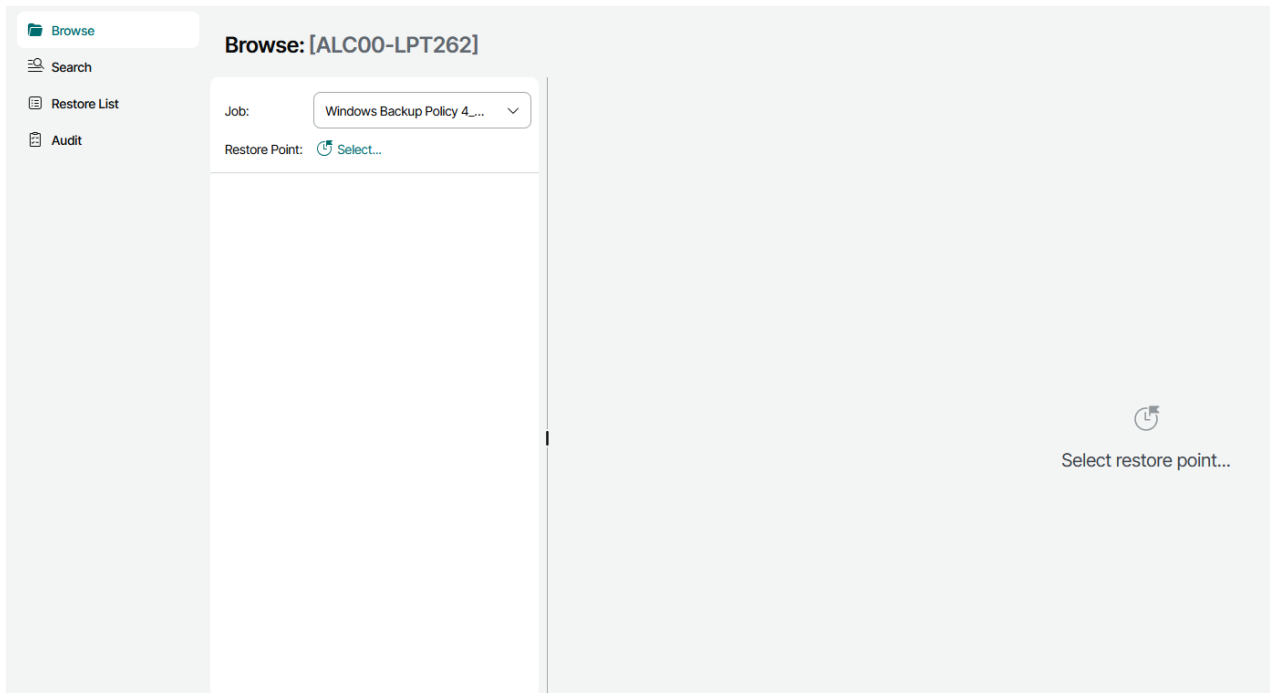
### Protected Data

Computer

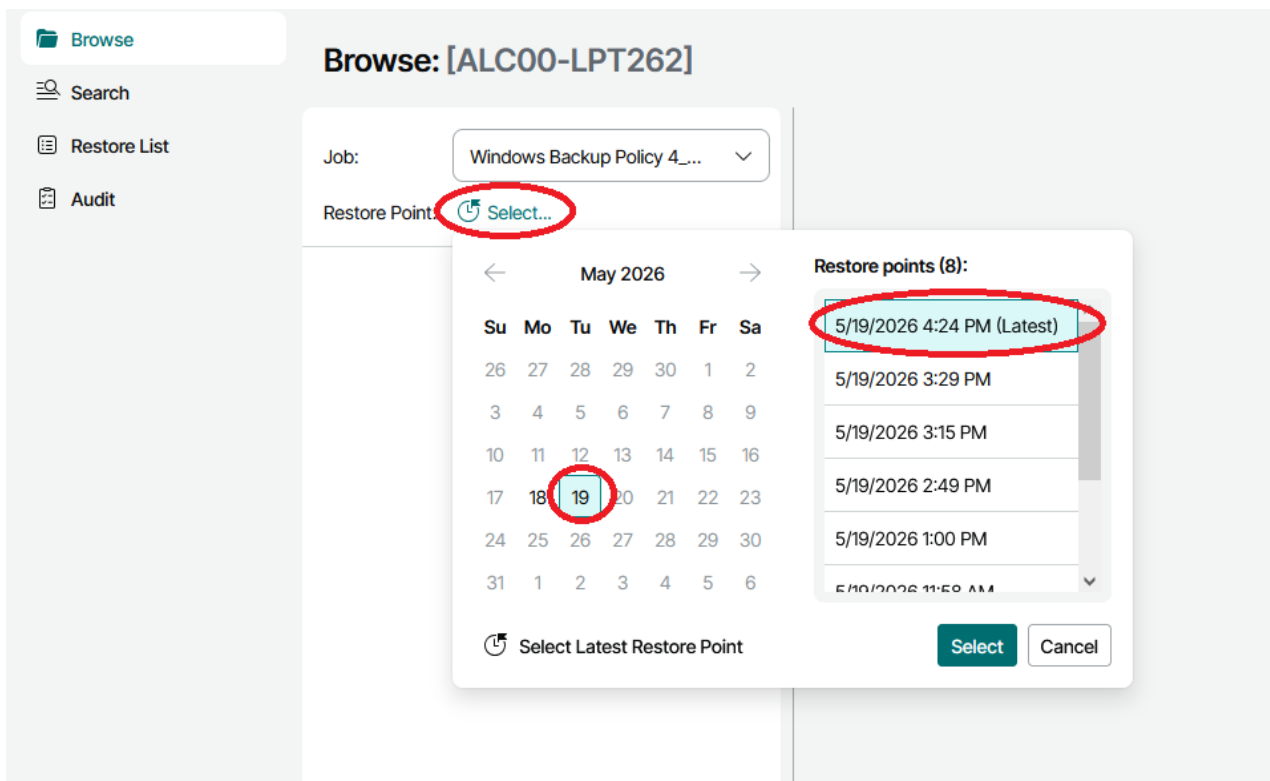
**File-Level Restore**

<input type="checkbox"/>	Name ↑	Backup Status	Tag	Backups	Backup Copies	Guest OS	Latest Restore Point	Cloud Copy	L
Selected: 1 of 2									
<input checked="" type="checkbox"/>	ALC00-LPT262	Active	Not set...	1	-	Microsoft Windo...	23 hours ago	Yes (23 hours ...	2
<input type="checkbox"/>	WinClient1	Orphaned	-	1	-	No info	1 day ago	Yes (1 day ago)	-

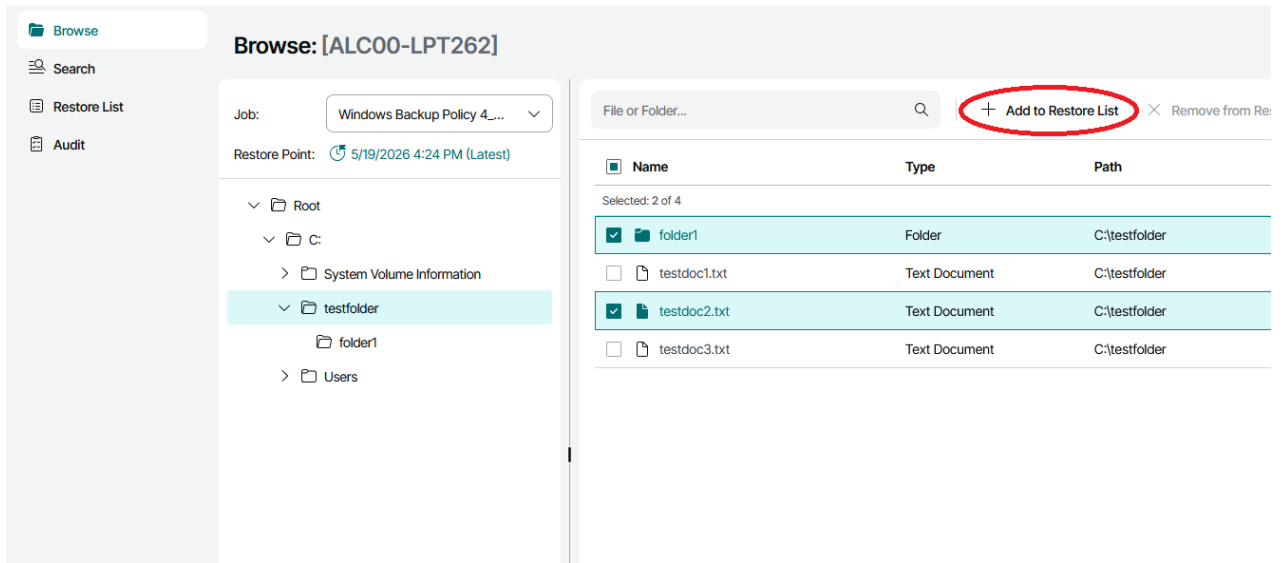
Isto leva-nos ao portal de restauro:



Aqui podemos escolher o backup job e o ponto de restauro pretendido:



Navegando pelo filesystem podemos seleccionar um ou mais ficheiros e/ou pastas a recuperar, adicionando-os à lista de restauro:



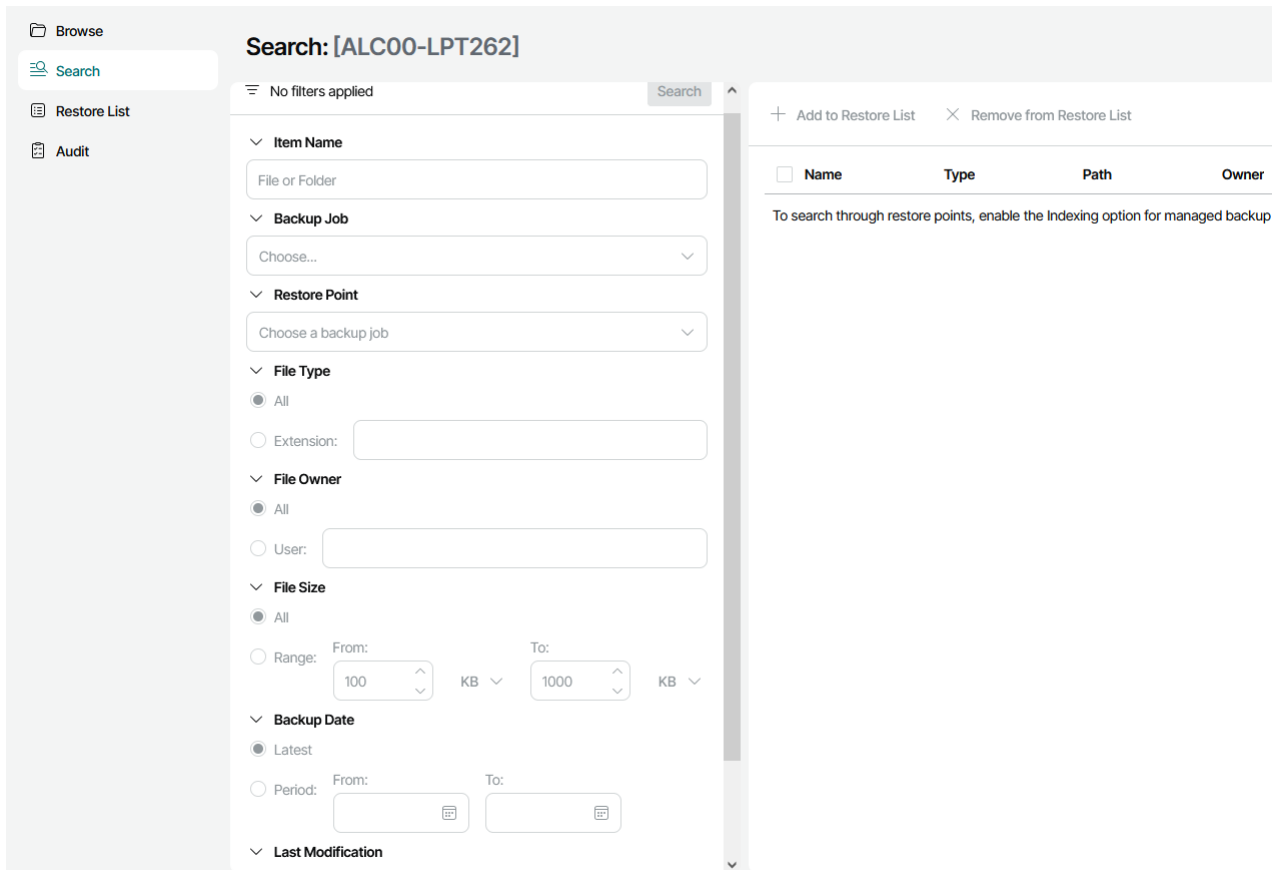
**Browse: [ALC00-LPT262]**

Job: Windows Backup Policy 4...  
Restore Point: 5/19/2026 4:24 PM (Latest)

File or Folder...  **+ Add to Restore List**

Name	Type	Path
<input checked="" type="checkbox"/> folder1	Folder	C:\testfolder
<input type="checkbox"/> testdoc1.txt	Text Document	C:\testfolder
<input checked="" type="checkbox"/> testdoc2.txt	Text Document	C:\testfolder
<input type="checkbox"/> testdoc3.txt	Text Document	C:\testfolder

Adicionalmente à navegação pelos pontos de restauro e sistema de ficheiros, é possível procurar por ficheiros no separador "Search":



**Search: [ALC00-LPT262]**

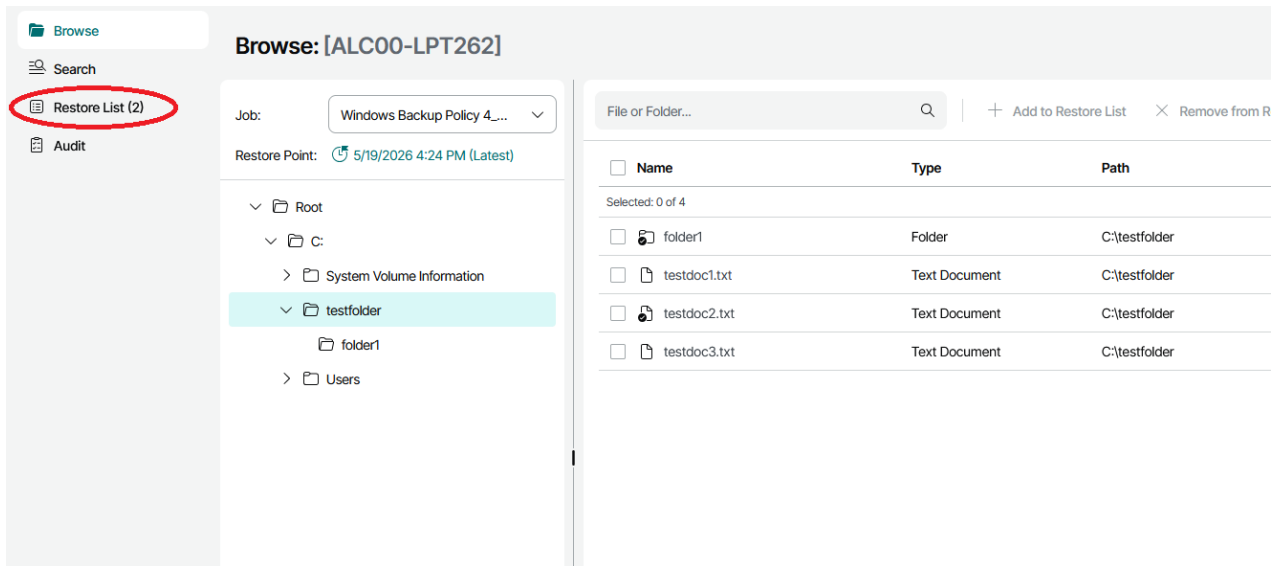
No filters applied

Name	Type	Path	Owner
To search through restore points, enable the Indexing option for managed backup			



Para que seja possível usar a funcionalidade de busca no portal é necessário que a indexação esteja ativa na configuração do backup job. Essa opção só está disponível no modo de operação **Servidor**.

Depois de adicionar os ficheiros pretendidos à lista, navega-se até ao separador "Restore List" na barra superior. O número que surge à frente é o número de ficheiros na lista:



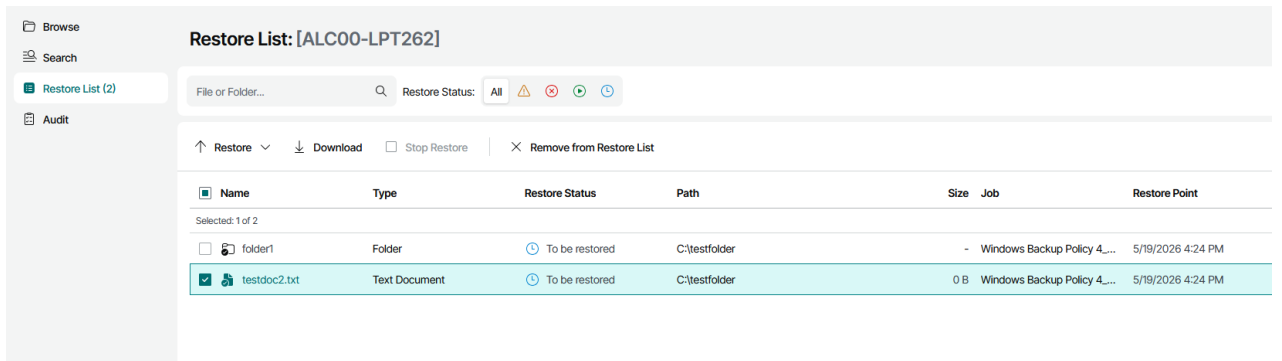
**Browse: [ALC00-LPT262]**

Job: Windows Backup Policy 4...  
Restore Point: 5/19/2026 4:24 PM (Latest)

File or Folder... | + Add to Restore List | X Remove from R

Name	Type	Path
Selected: 0 of 4		
<input type="checkbox"/> folder1	Folder	C:\testfolder
<input type="checkbox"/> testdoc1.txt	Text Document	C:\testfolder
<input type="checkbox"/> testdoc2.txt	Text Document	C:\testfolder
<input type="checkbox"/> testdoc3.txt	Text Document	C:\testfolder

Aí temos a opção de remover, recuperar todos os ficheiros ou recuperar apenas alguns.



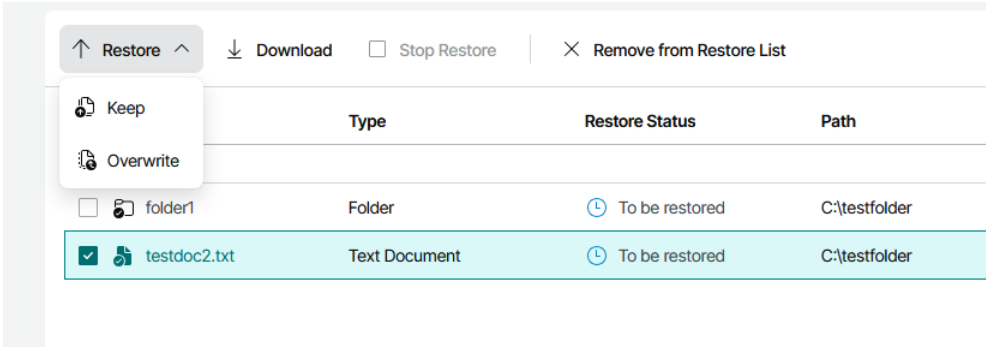
**Restore List: [ALC00-LPT262]**

File or Folder... | Restore Status: All | [Warning] [Error] [Refresh] [Undo]

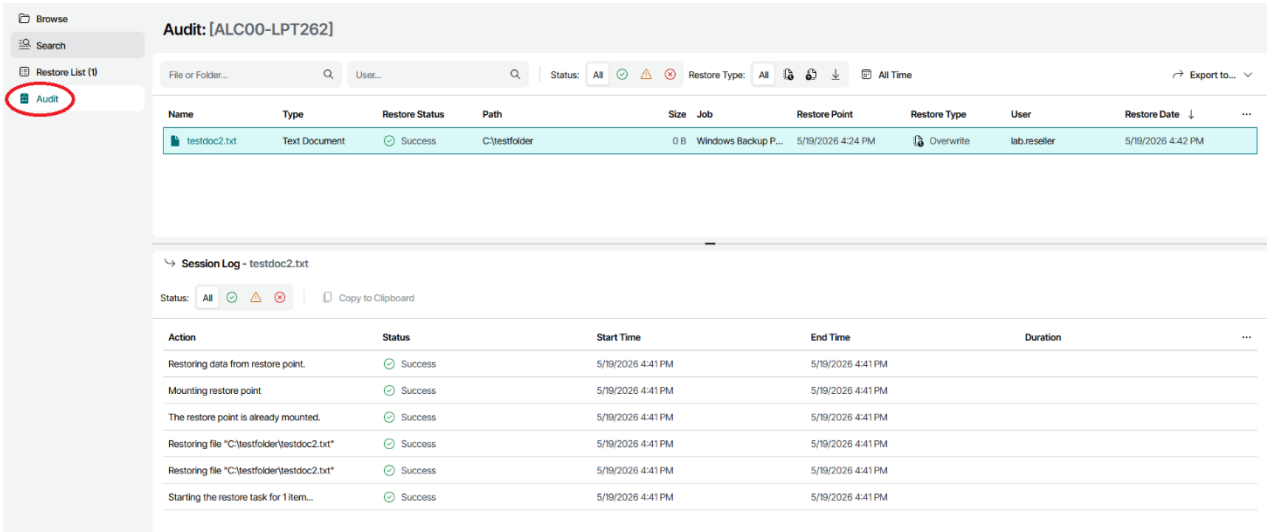
↑ Restore | ↓ Download | Stop Restore | X Remove from Restore List

Name	Type	Restore Status	Path	Size	Job	Restore Point
Selected: 1 of 2						
<input type="checkbox"/> folder1	Folder	To be restored	C:\testfolder	-	Windows Backup Policy 4...	5/19/2026 4:24 PM
<input checked="" type="checkbox"/> testdoc2.txt	Text Document	To be restored	C:\testfolder	0 B	Windows Backup Policy 4...	5/19/2026 4:24 PM

O método de recuperação pode ser por Download para a máquina que se está a usar para aceder ao portal, restaurar para a pasta original substituindo o que lá está ("Overwrite"), ou restaurar para a pasta original, mas criando uma cópia do ficheiro ("Keep"):



Na opção "Audit" é possível verificar o que foi restaurado, quando, que utilizador o fez e qual o método:



### 3.11 Recuperação completa da máquina

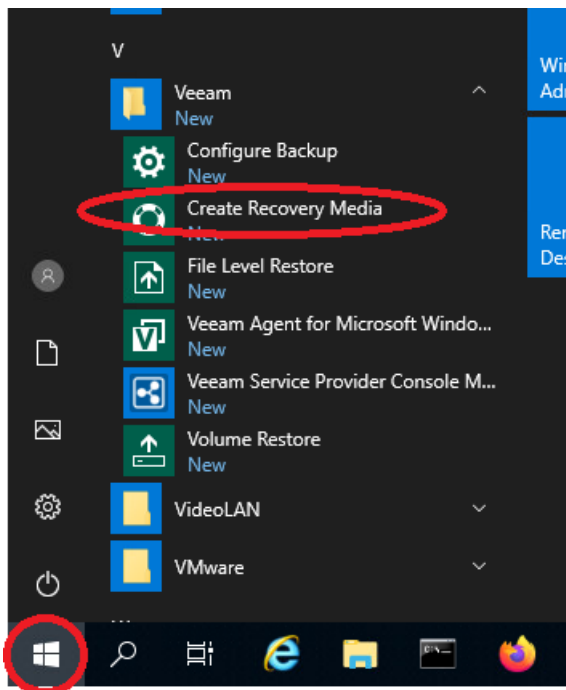
#### 3.11.1 Criação do meio de recuperação em máquinas Windows

Para que seja possível a recuperação completa da máquina é conveniente criar antecipadamente um meio de recuperação.

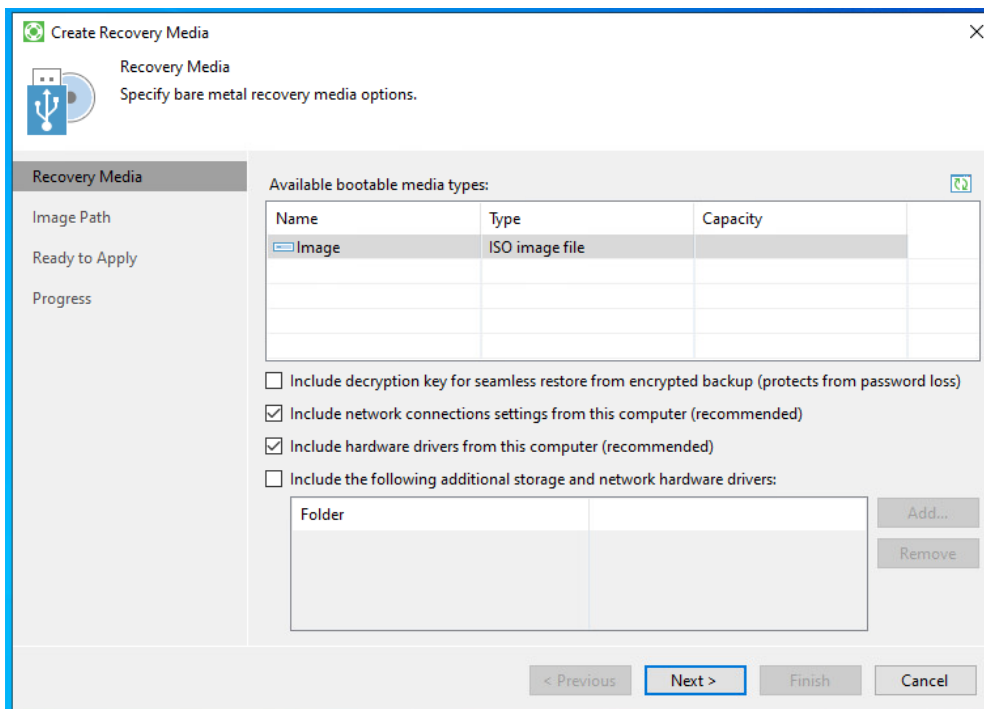
Para isso, para cada máquina passível de recuperação total, deve-se aceder à aplicação "Create Recovery Media".



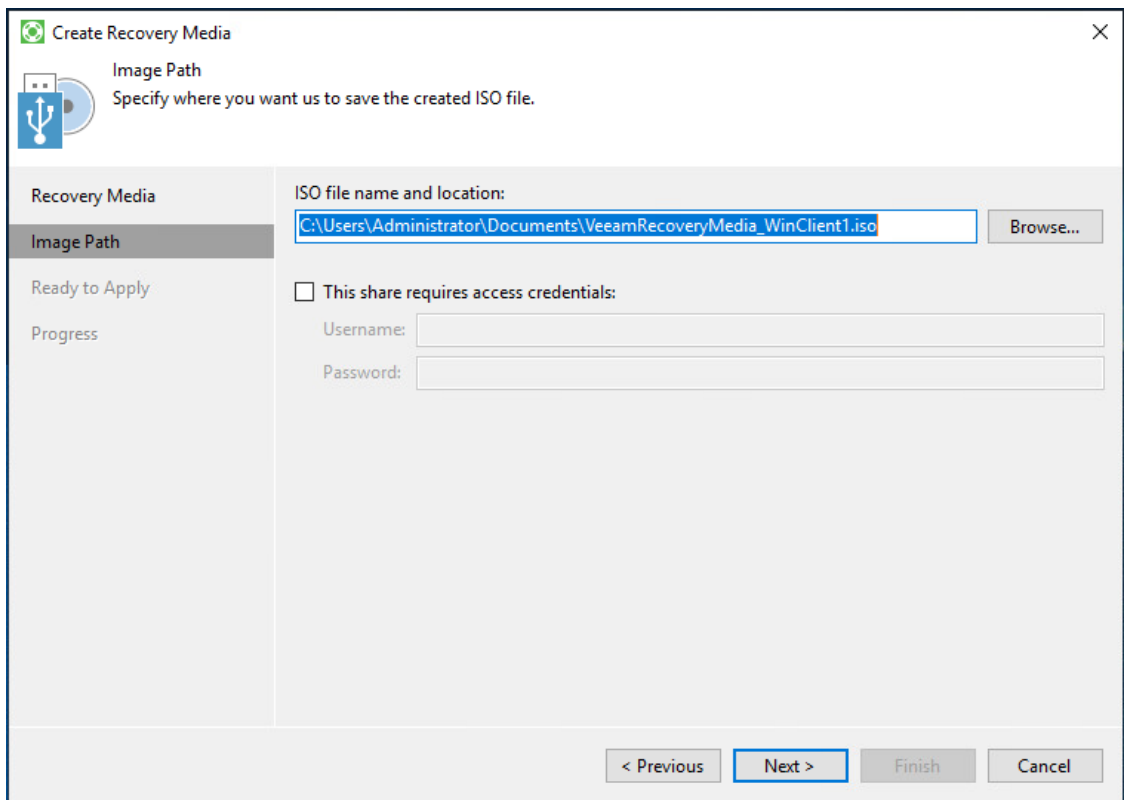
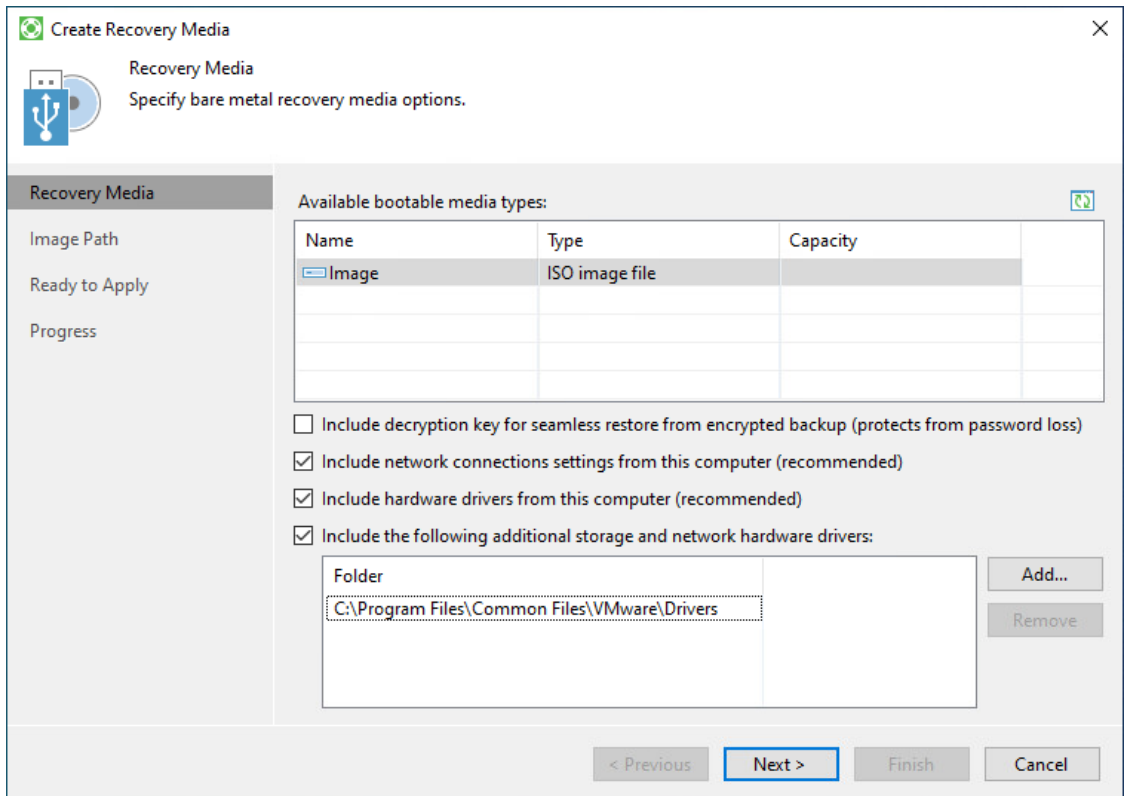
Existe um problema conhecido com *Recovery Medias* criados a partir de Windows Server 2022. O *Recovery Media* pode falhar durante o boot ou apresentar erros de certificado SSL mais à frente. Recomenda-se que se use outra versão de Windows para o criar.



O processo é bastante simples, como se pode ver nos quadros seguintes.



Podem-se adicionar drivers por forma a garantir a operacionalidade da máquina recuperada no ambiente destino. Por exemplo, para garantir que uma máquina recuperada num ambiente vmware tenha acesso aos drivers das placas de rede virtuais, gráficas e etc, deve-se adicionar o path onde estes se encontram na máquina atual:





A partir deste momento pode encontrar o ISO do meio criado na pasta definida anteriormente. Deve guardar o mesmo por forma a utilizá-lo para fazer boot à máquina quando necessário.

### 3.11.2 Criação do meio de recuperação em máquinas Linux

Para que seja possível a recuperação completa de máquinas Linux, é necessário um meio de recuperação baseado em Linux.

Pode ser usado um meio genérico, que pode ser solicitado à Ar.

### 3.11.3 Recuperação com base no Recovery Media Windows

Fazendo boot com o meio de recuperação criado anteriormente, surge uma primeira janela com opções de configuração da ferramenta e de recuperação.



É necessário garantir que os drivers Windows estão carregados para a máquina que se pretende recuperar. Na janela inicial pode-se verificar se os drivers de rede estão carregados (no caso apresentado não estão) e pode-se fazê-lo carregando em cima do ícone de rede.



---


Existe um problema conhecido com *Recovery Medias* criados a partir de Windows Server 2022. O *Recovery Media* pode falhar durante o boot ou apresentar erros de certificado SSL mais à frente. Recomenda-se que se use outra versão de Windows para o criar.

---

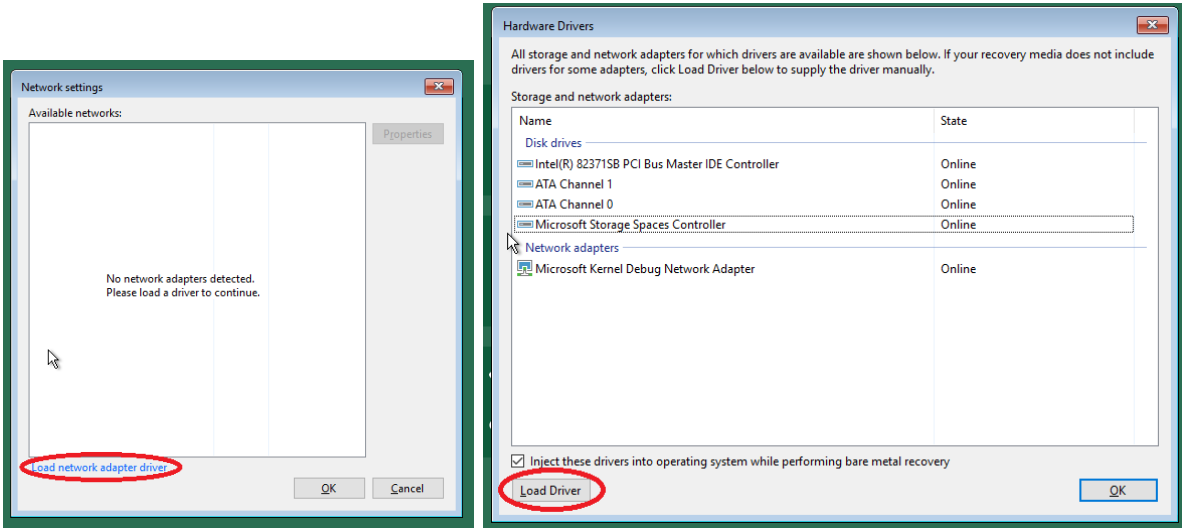
# Veeam Recovery Media 13.0.2

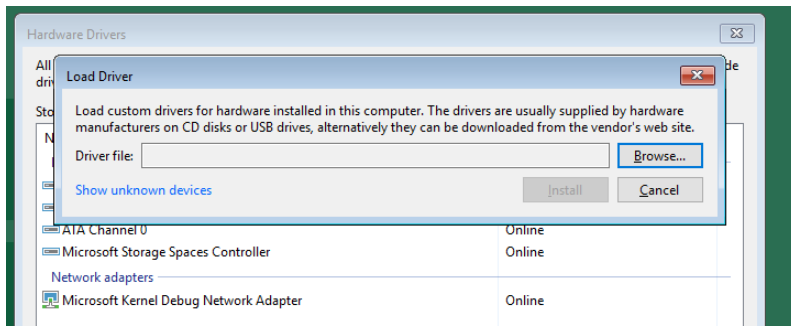
Created from Microsoft Windows Server 2019 (1809, 64-bit)

- Bare Metal Recovery**  
Restore Veeam Agent for Windows backup to the original or a new computer.
- Windows Recovery Environment**  
Launch Microsoft Windows system image recovery environment.
- Tools**  
Browse tools for system management and diagnostics.

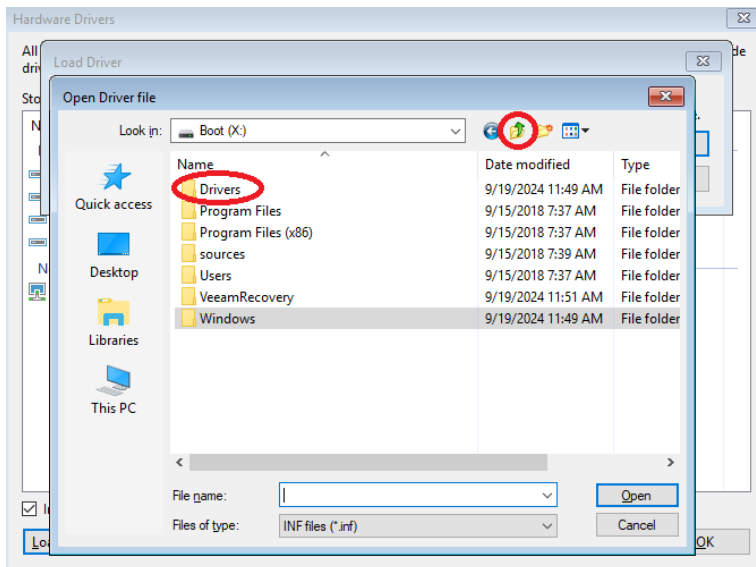


Vai aparecer uma janela com informação das redes e onde permite a configuração dos drivers:

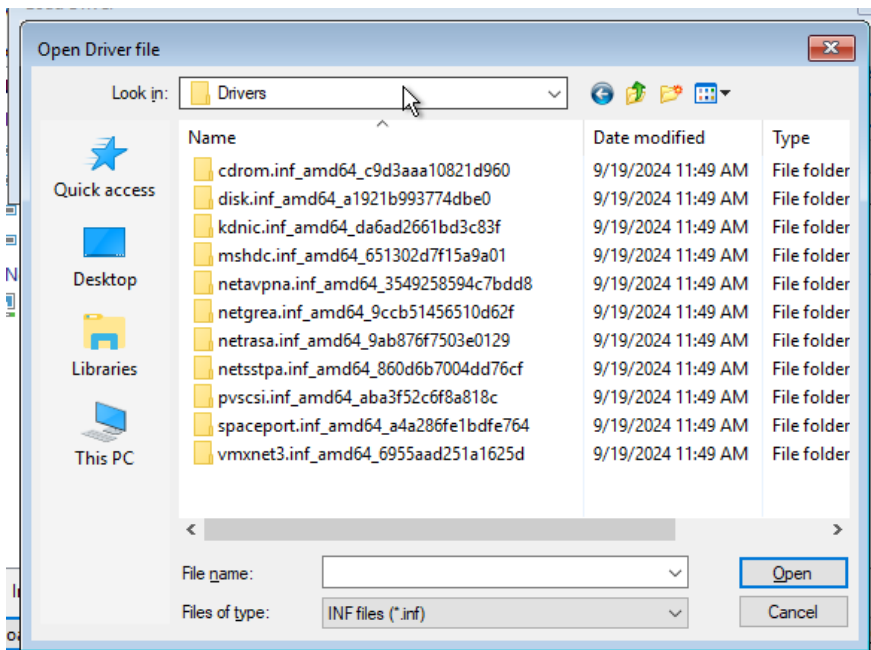




Navegar até à pasta de "Drivers":

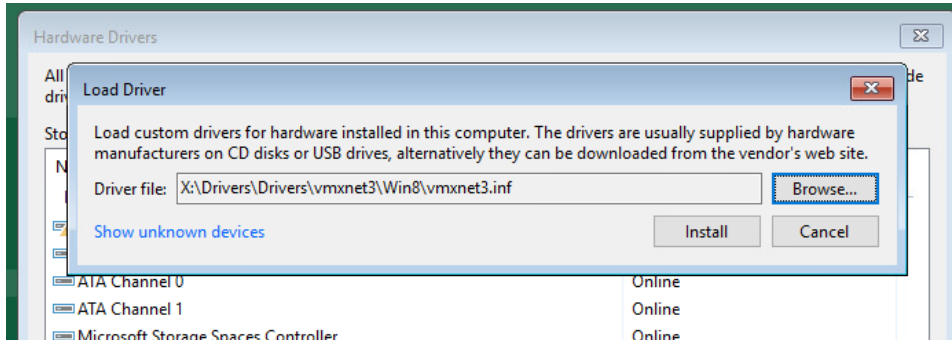


E escolher o driver em conformidade:

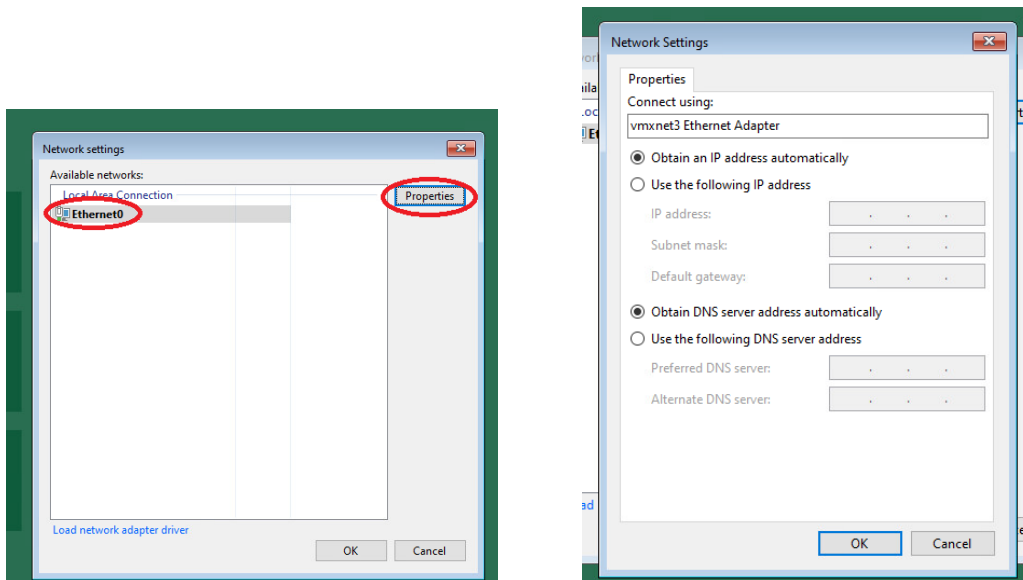




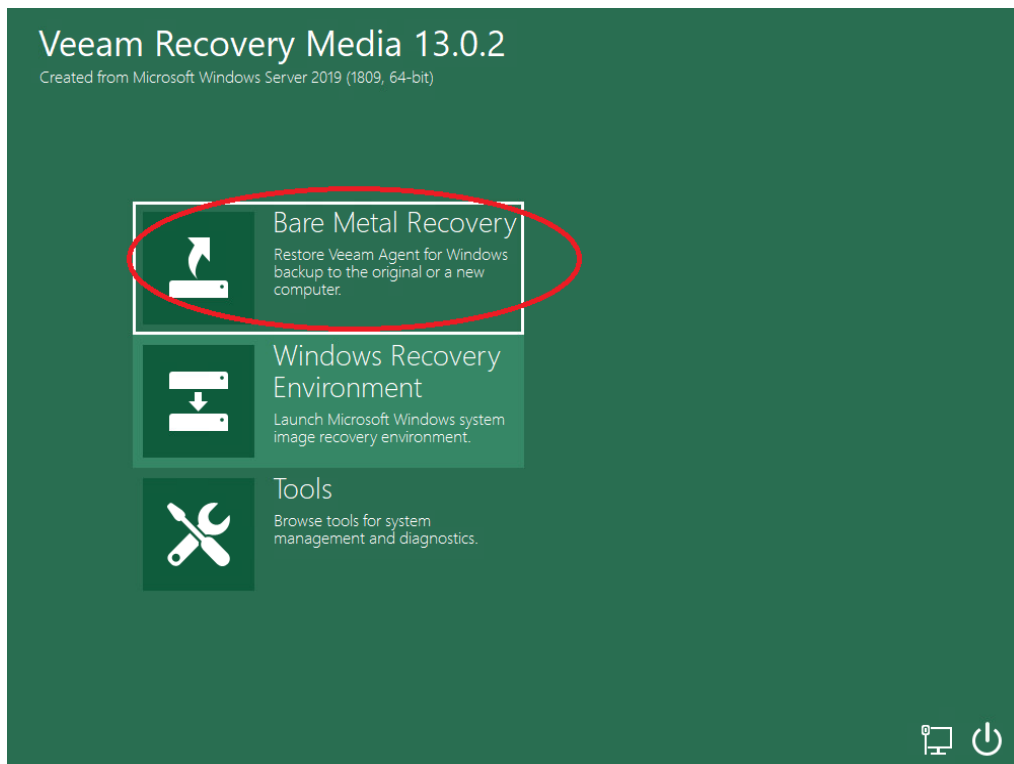
No caso de se estar a recuperar para uma máquina que não a original, é necessário criar um *Media Recovery* que inclua os drivers necessários para esta nova máquina de destino.



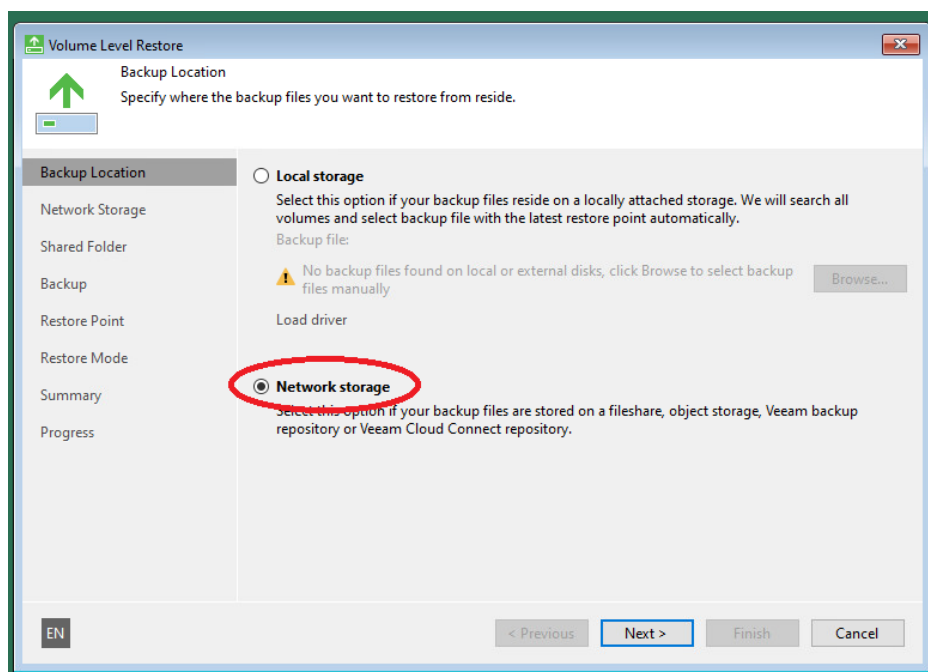
Depois do driver de rede instalado, verifica-se a configuração de rede e altera-se em conformidade:



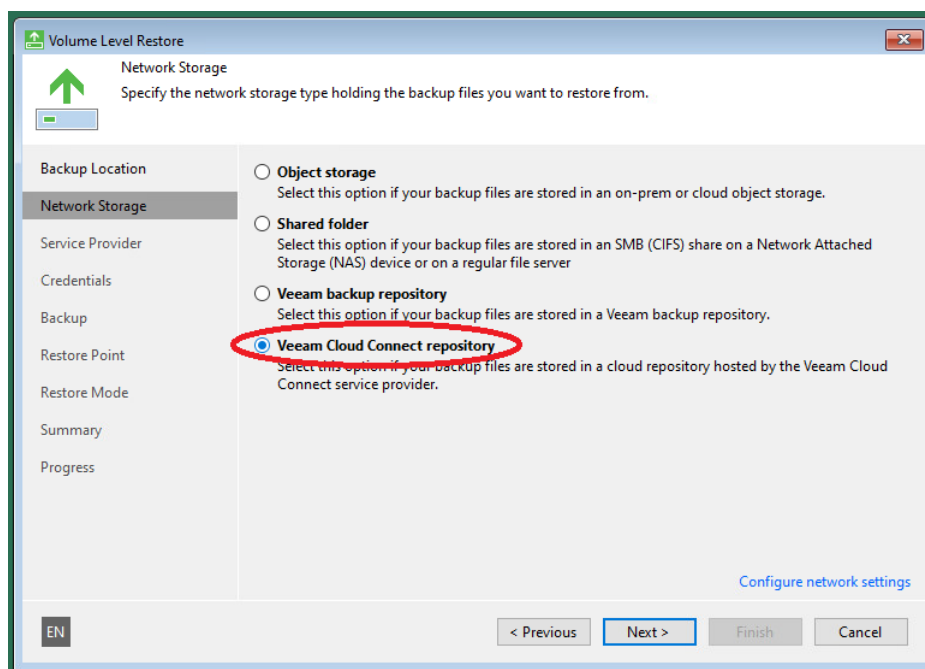
Depois de corretamente configurado, pode-se verificar que o ícone de rede não apresenta indicação de erro. Pode ainda ser necessário instalar outros drivers (por exemplo de disco/storage). Assim que todos os drivers estiverem instalados, pode-se prosseguir para a recuperação Bare Metal.



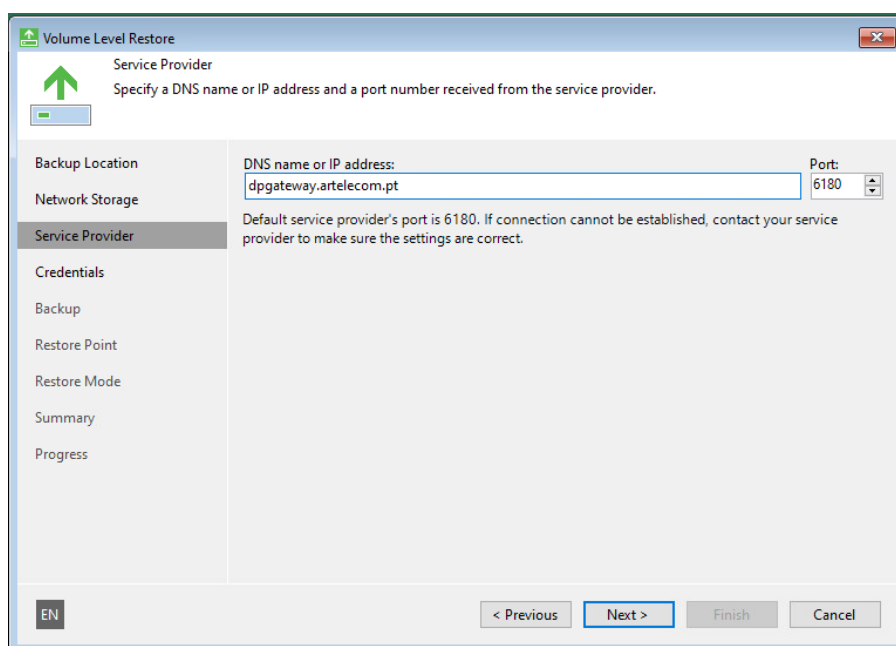
Como pretendemos recuperar a máquina com um backup do repositório da Ar, escolhemos "Network storage" como localização:



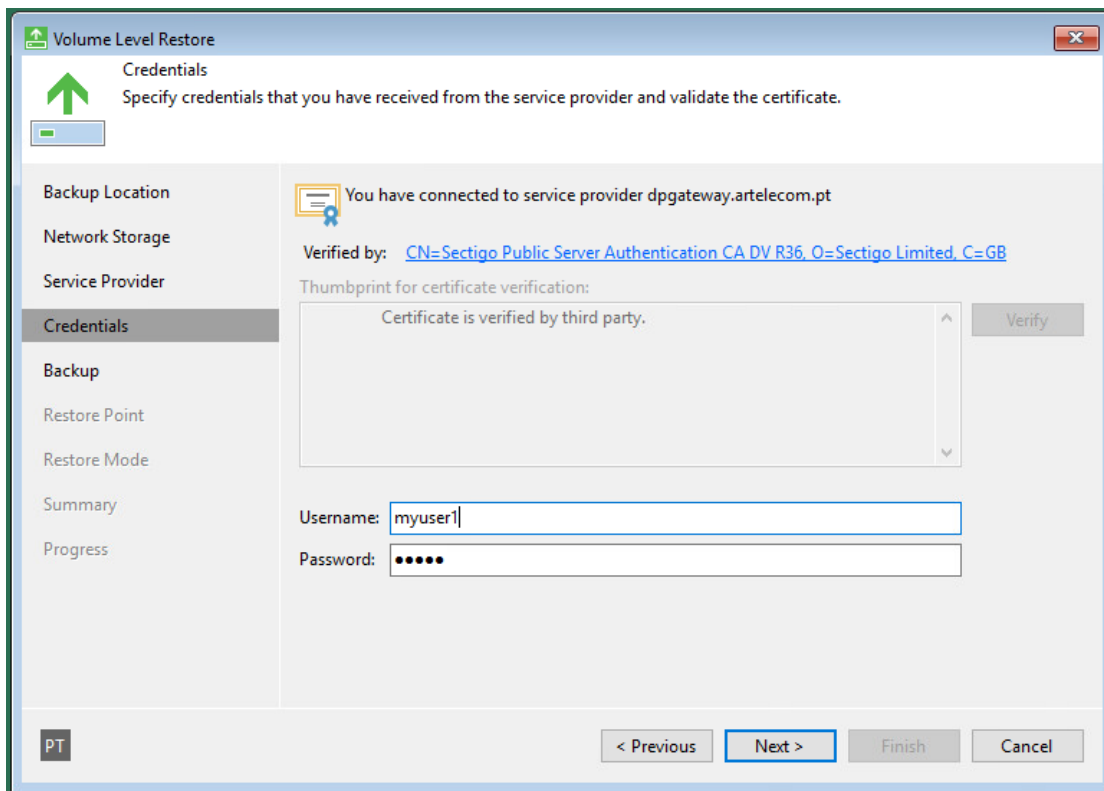
e "Veeam Cloud Connect repository"



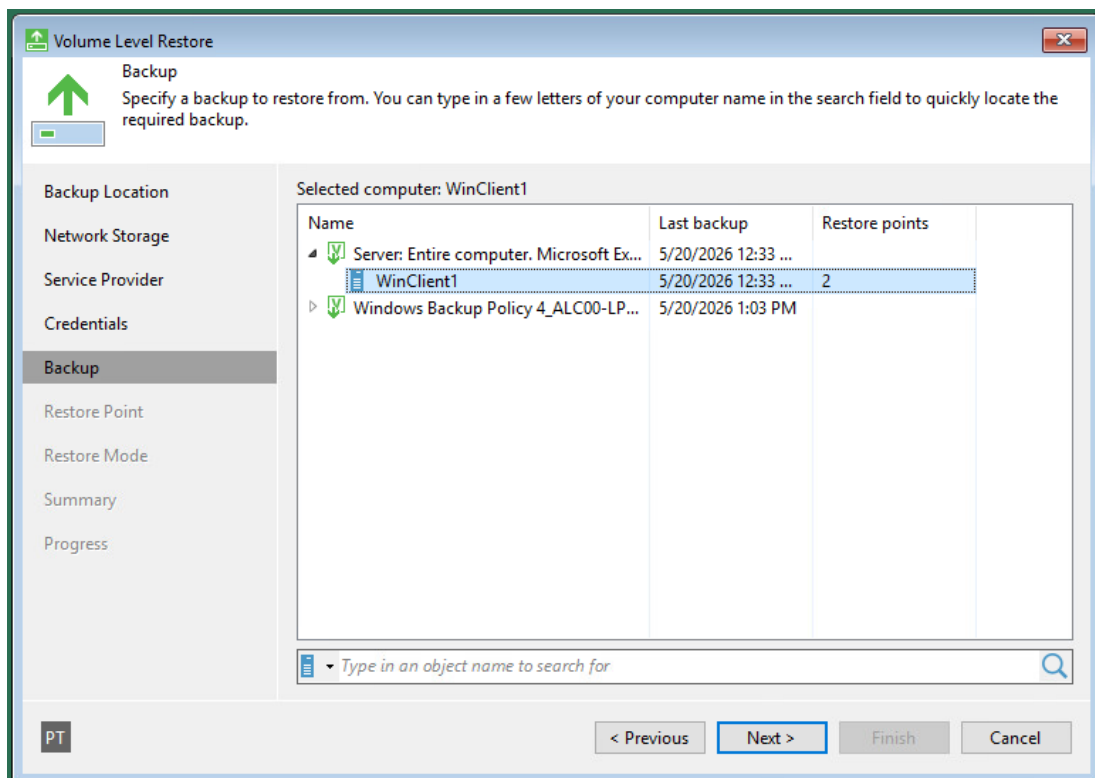
O próximo passo é introduzir o endereço da gateway da Ar que foi enviado no email de boas-vindas (por defeito usar **dpgateway.artelecom.pt** na porta **6180**):



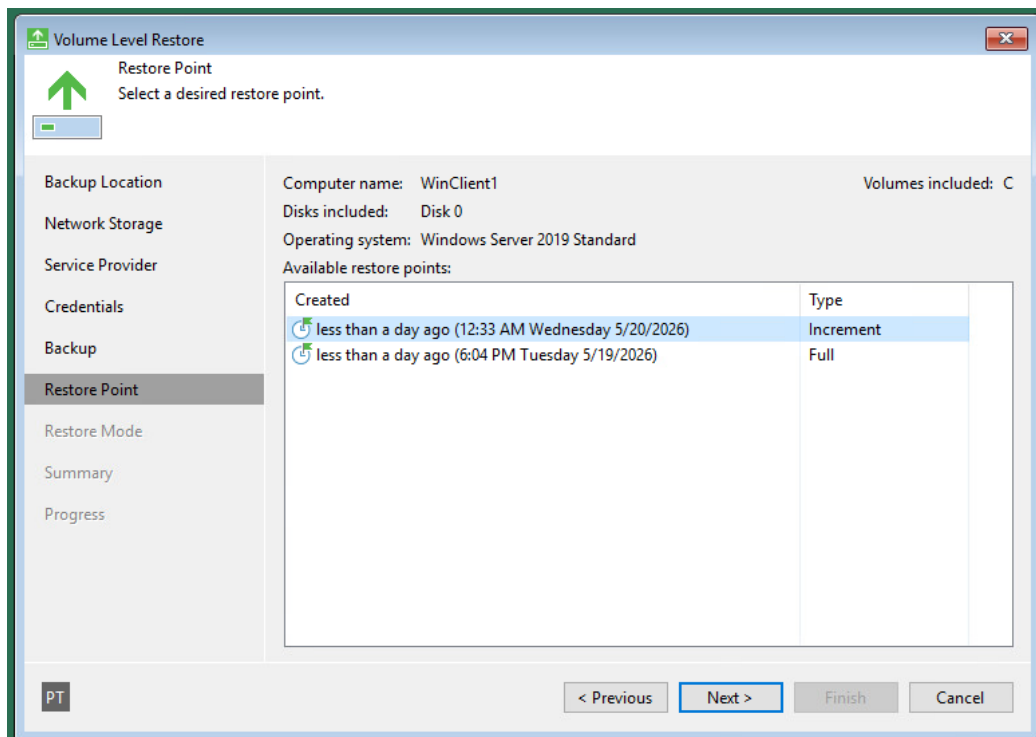
Depois de verificado o certificado SSL, é solicitada a introdução das credenciais de acesso do utilizador owner da companhia de onde se está a recuperar e enviadas pela Ar no email de boas vindas.



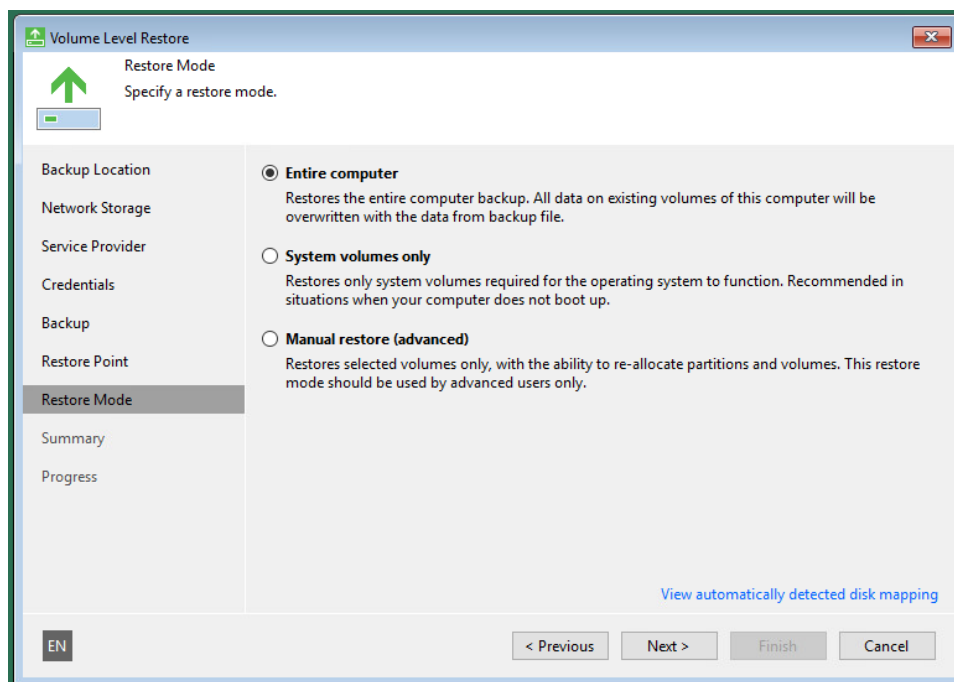
e após corretamente autenticado, podemos escolher qual o backup a recuperar:



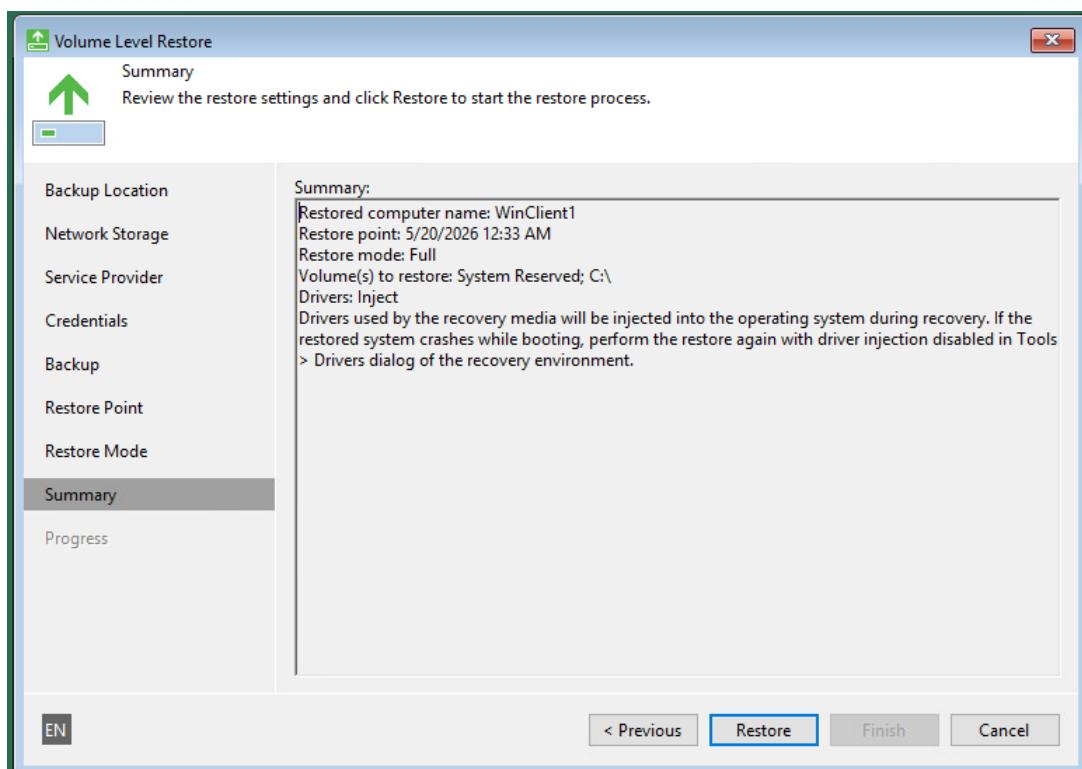
qual o ponto de restauro e avançar carregando em "Next":



No quadro seguinte temos a opção de recuperar a máquina completa ou apenas alguns volumes. Para este exemplo, vamos recuperar a máquina completa.



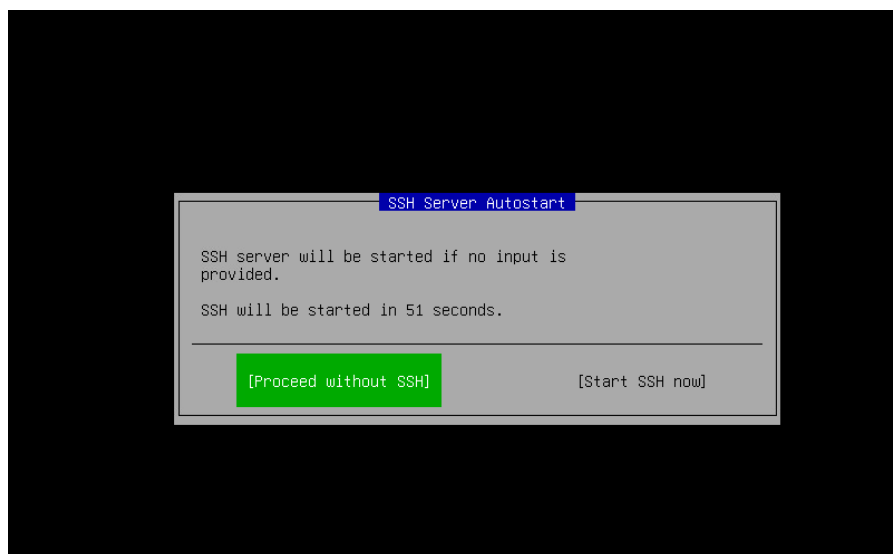
Se a máquina onde vai ser feito o restauro completo tiver partições no disco, pode ser necessário fazer o mapeamento manual das partições restauradas. Se o disco estiver limpo, o Veeam criará as partições tal como estavam na máquina original.



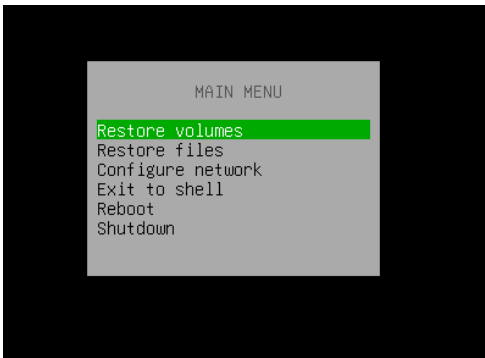
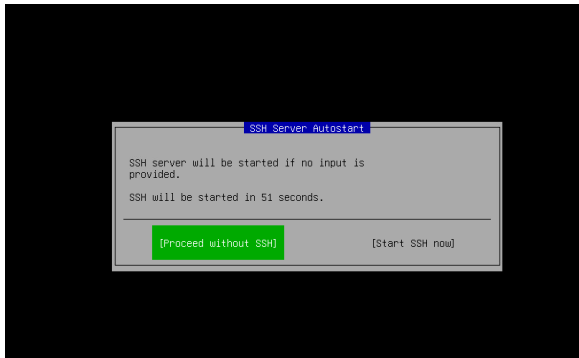
Depois do processo concluído, retirar o *Recovery Media* do boot e reiniciar a máquina.

### 3.11.4 Recuperação com base no Recovery Media Linux

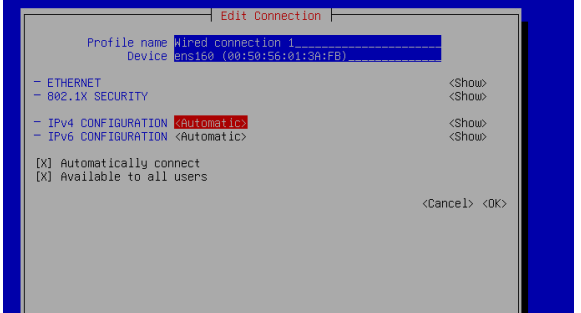
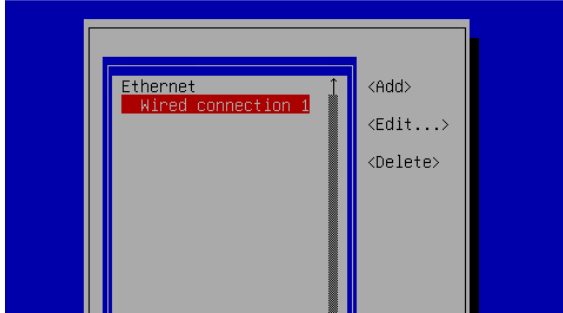
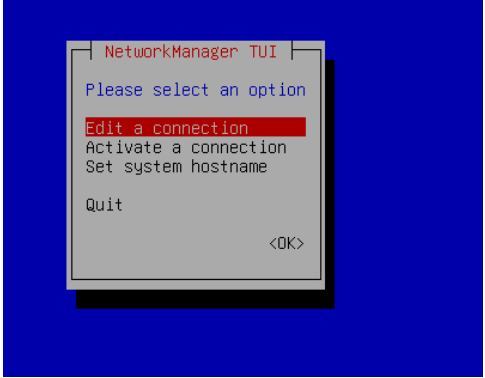
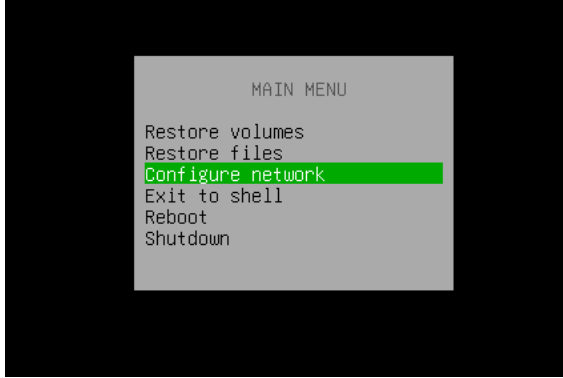
Ao fazer boot por este meio, surge um quadro dando a opção de iniciar o serviço SSH caso se pretenda fazer a recuperação remotamente.

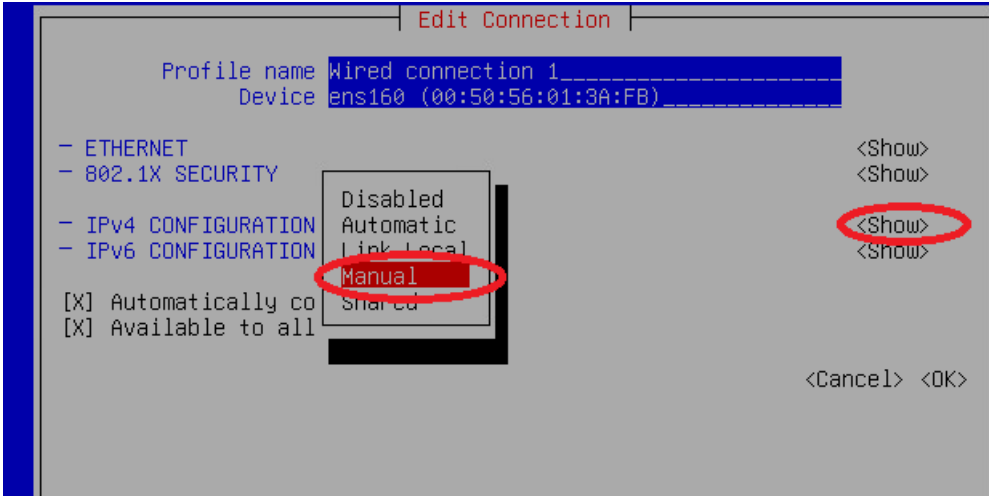


Continuando na consola, o próximo passo é aceitar os termos do licenciamento seguindo-se o menu de recuperação:

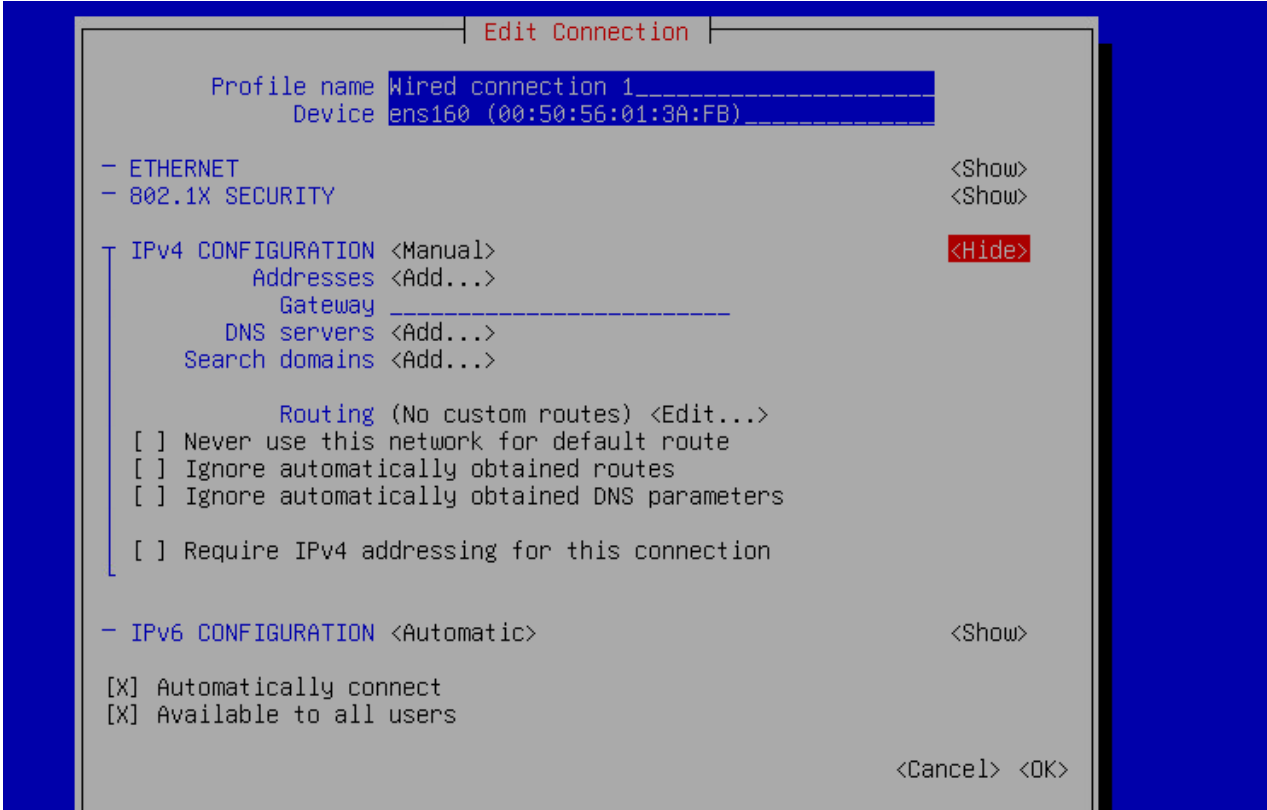


Para recuperar a máquina a partir do repositório da Ar é necessário garantir que a conectividade de rede esteja ativa e, portanto, é necessário configurar a rede:

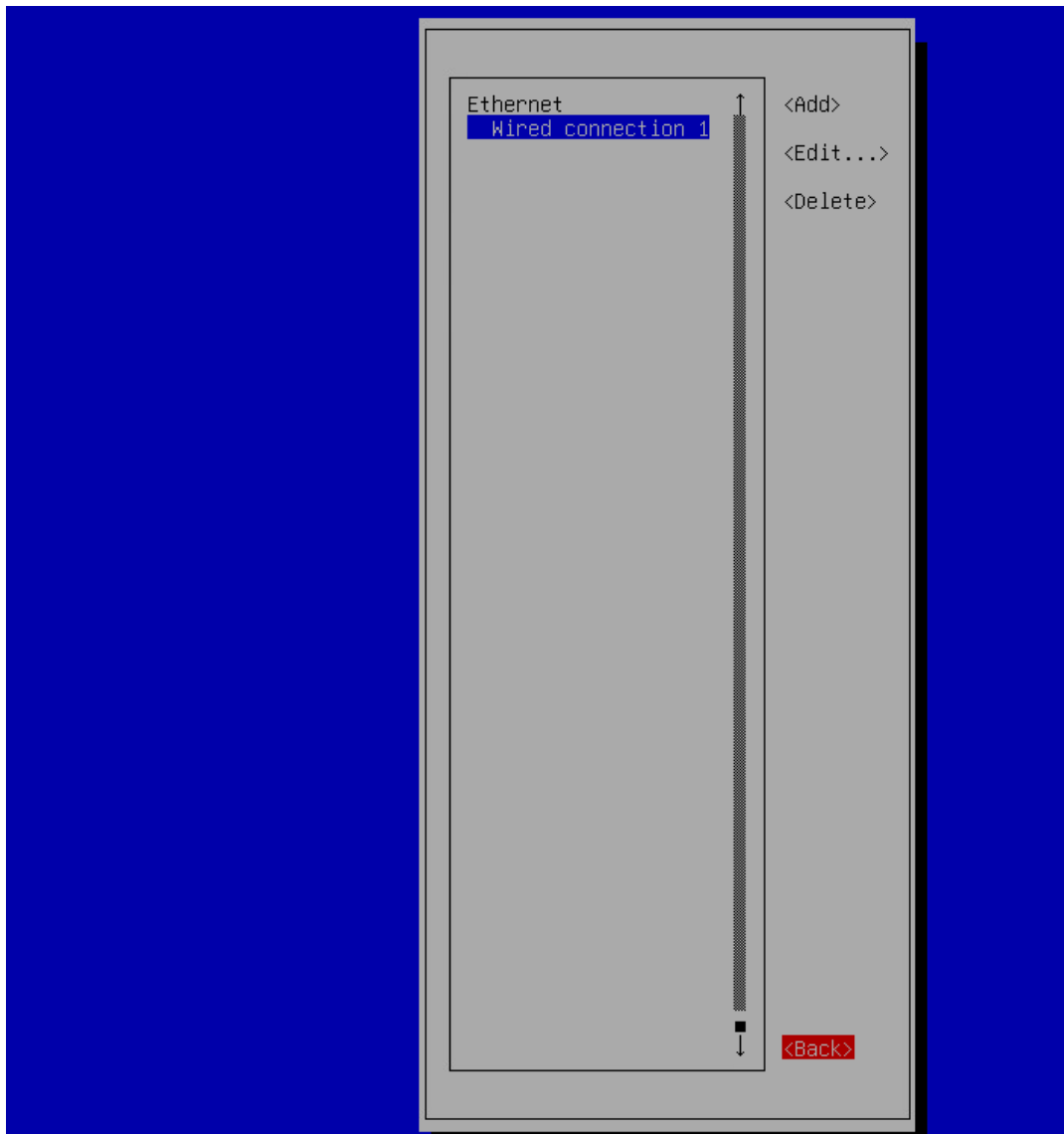




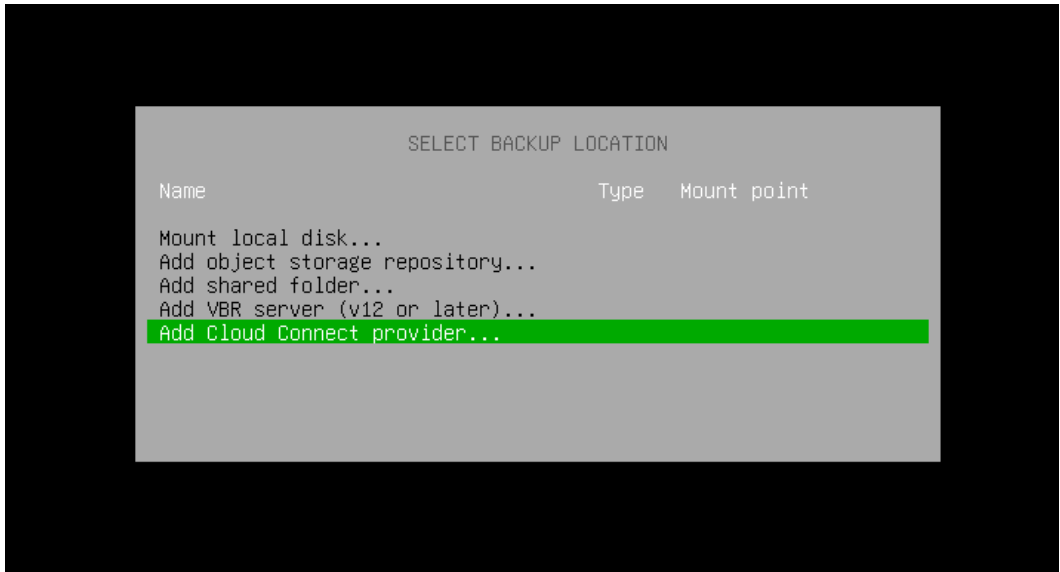
Configurar a rede em conformidade e fazer <OK>:



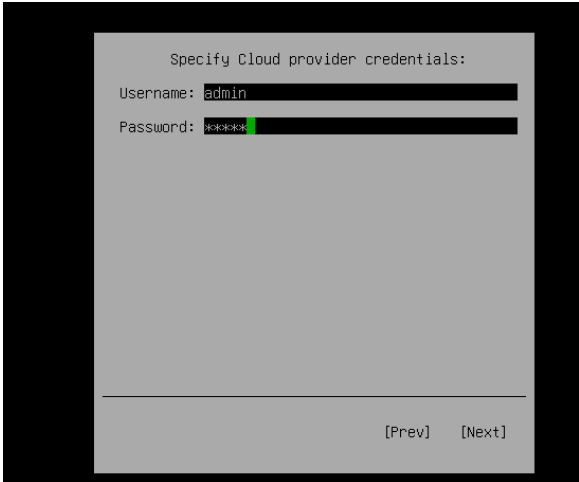
No quadro que vai aparecer fazer <Back>



A partir deste momento é possível restaurar ficheiros ou volumes completos. Para isso selecionar a opção pretendida e escolher a localização do backup a recuperar. Neste caso, escolher *"Add Cloud Connect provider..."*



Configurar com a informação recebida no email de Boas-Vindas e introduzir as respetivas credenciais:



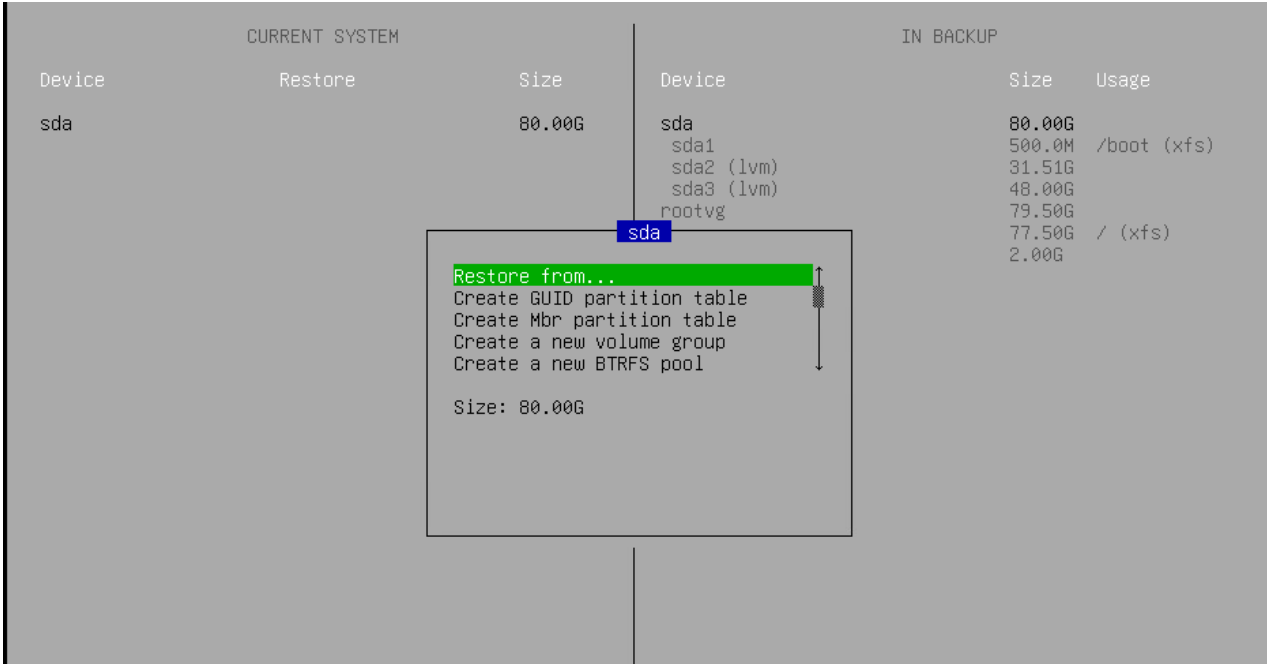
A partir daqui é possível escolher o backup e qual o ponto de restauro a recuperar:

IMPORTED BACKUPS			RESTORE POINTS
Job name	Hostname	Points	Created at
Linux server - Entire computer_LAB1-LNXSRV02 - LAB1-LNX...	LAB1-LNXSRV02	7	00:30 17-09-2024 00:30 16-09-2024 00:30 15-09-2024 00:30 14-09-2024 00:30 13-09-2024 00:30 12-09-2024 17:03 11-09-2024

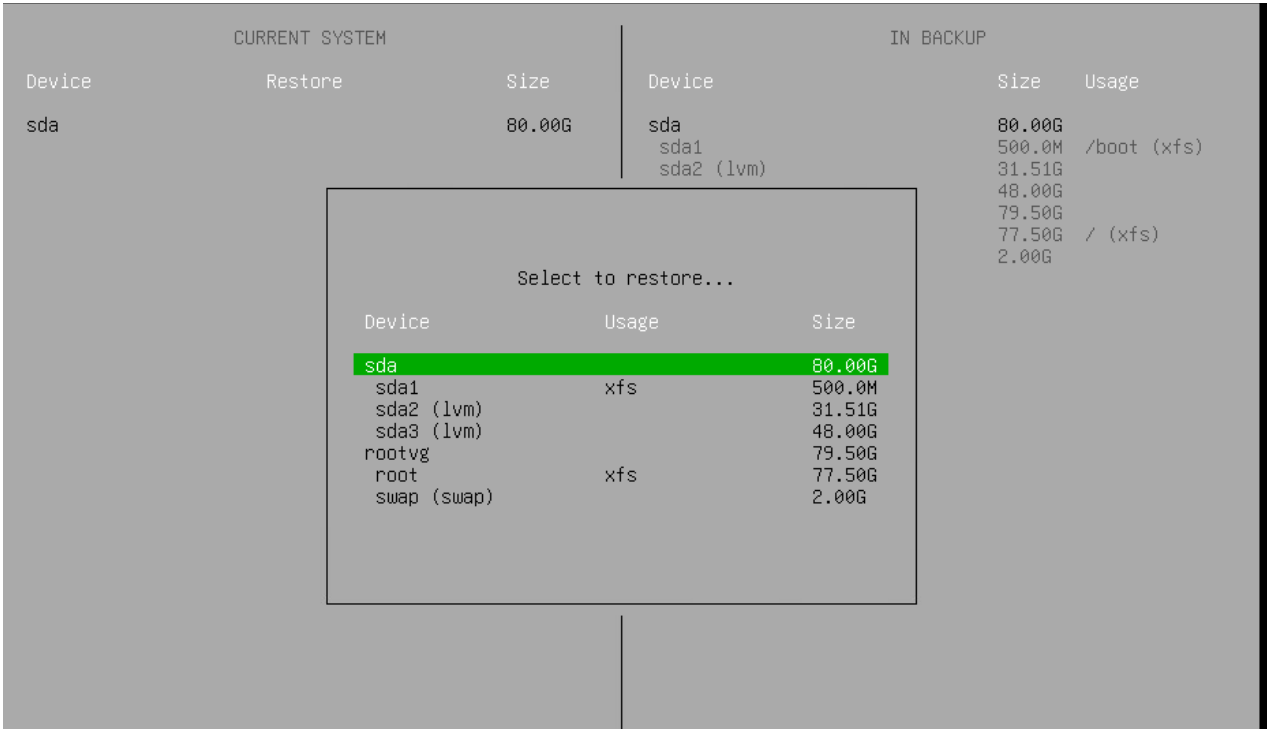
E quais os volumes:

CURRENT SYSTEM			IN BACKUP		
Device	Restore	Size	Device	Size	Usage
sda		80.00G	sda	80.00G	
			sda1	500.0M	/boot (xfs)
			sda2 (lvm)	31.51G	
			sda3 (lvm)	48.00G	
			rootvg	79.50G	
			root	77.50G	/ (xfs)
			swap (swap)	2.00G	

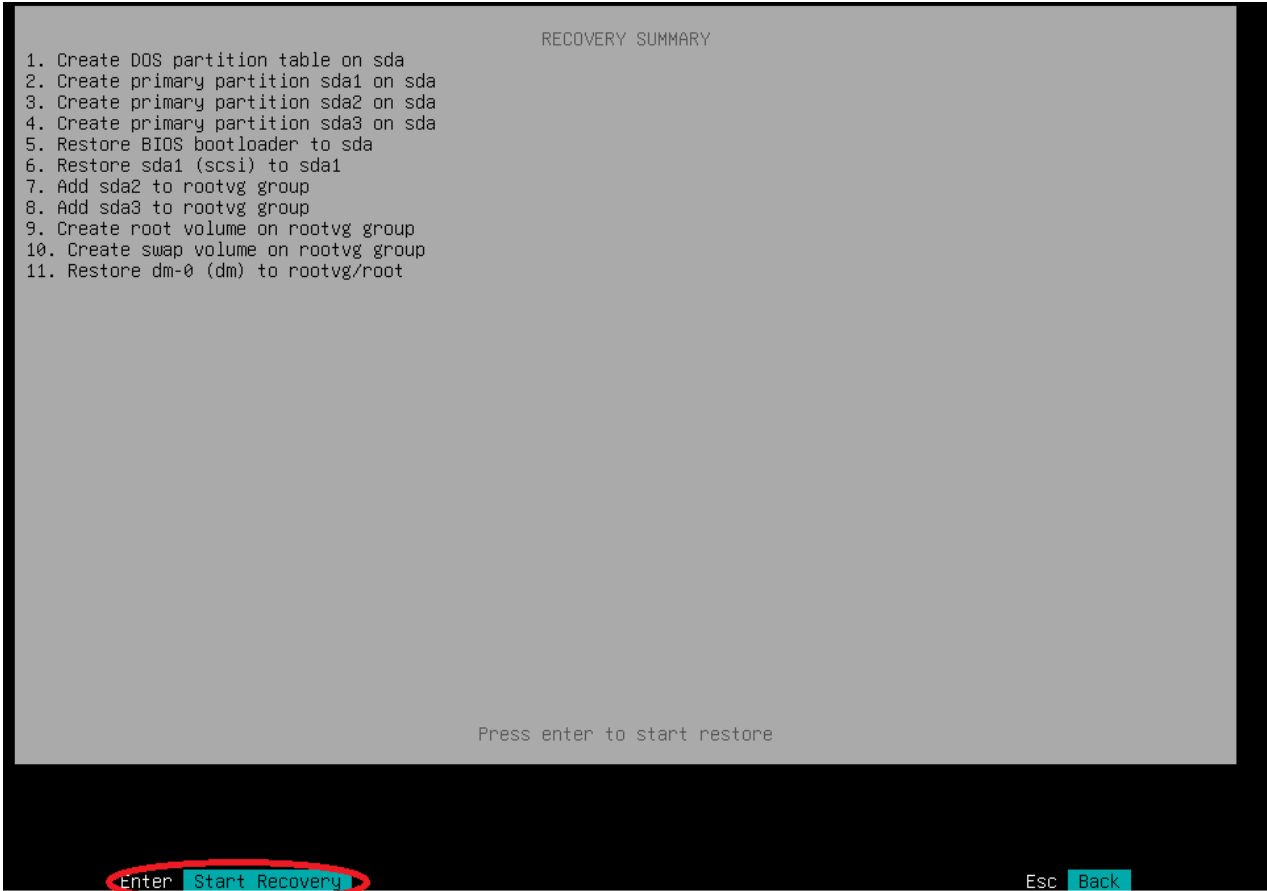
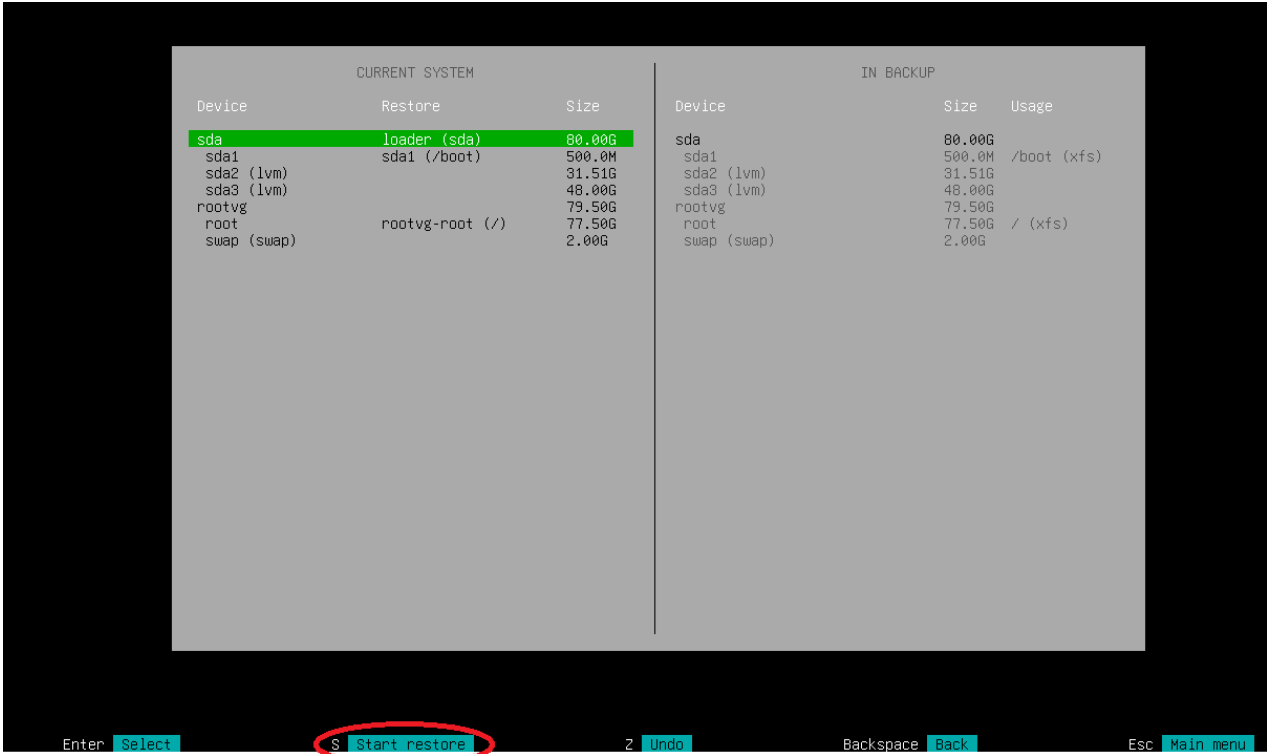
Selecionar o dispositivo pretendido (neste caso sda) e escolher "Restore from...":



Escolher a opção pretendida



e carregar em "S" para iniciar o restauro, seguido de *Enter*:



O processo vai iniciar e assim que concluído fazer "ESC" para voltar ao menu principal e fazer reboot.

```

Veeam Recovery Media

Restore 100% Status: Success

Time Action Duration
13:52:50 Job started at 2024-09-17 13:52:50 UTC
13:52:52 Starting volume restore
13:53:03 Applying changes to disks configuration 00:00:12
13:53:15 rootvg-root restored 77.5 GB at 21.4 MB/s 01:01:48
14:55:03 sdal restored 500 MB at 17.1 MB/s 00:00:29
14:55:32 Restoring bootloader on /dev/sda 00:00:01
14:55:39 Processing finished at 2024-09-17 14:55:39 UTC
14:57:26 Repository does not support log export
14:57:26 Logs have been exported to a local directory: /var/log/veeam/veeam_logs_val_20240917_145552.tar.gz

Esc Main menu

```

### 3.12 Recuperação de itens aplicativos

A recuperação de itens aplicativos é efetuada através de vários utilitários Veeam denominados **Veeam Explorer**.

Estes permitem a recuperação granular de:

- Active Directory
- Exchange
- MongoDB
- Oracle
- PostgreSQL
- SAP HANA
- SharePoint
- MSSQL
- Teams

Esta funcionalidade apenas está disponível para o cliente se o mesmo tiver um servidor Veeam Backup & Replication nas suas instalações. Em alternativa, pode solicitar à Ar a recuperação dos itens pretendidos.