

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[®]

CLOUD - Data Protection

Veeam Service Provider Console

MANUAL DE UTILIZADOR - PARCEIROS

Referência: M_GP_301

Data: 20/05/2026

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 | 20-05-2026 | 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 | 6 |
| 2. | ACESSO | 7 |
| 3. | CONFIGURAÇÃO DE RESELLER | 8 |
| 3.1 | Perfil do reseller | 8 |
| 3.2 | Branding | 9 |
| 3.3 | Notificações | 10 |
| 3.4 | Autenticação Multi-Factor (MFA) | 11 |
| 3.5 | Configuração de tarifários (planos de subscrição) | 14 |
| 3.6 | Gestão de utilizadores do Reseller | 15 |
| 4. | GESTÃO DE COMPANHIAS PELO RESELLER | 19 |
| 4.1 | Criar companhia | 20 |
| 4.1.1 | User Info | 21 |
| 4.1.2 | Configuração de serviços associados à companhia | 22 |
| 4.1.3 | Billing | 22 |
| 4.1.4 | Multi-Factor Authentication | 23 |
| 4.1.5 | Notificações | 23 |
| 4.2 | Criação e gestão de Tenants | 24 |
| 4.2.1 | Serviços | 26 |
| 4.2.2 | Bandwidth | 28 |
| 4.3 | Gestão de Localizações | 29 |
| 4.4 | Gestão de Utilizadores | 31 |
| 4.5 | Gestão de Serviços | 36 |
| 4.6 | Agente de Gestão | 37 |
| 4.7 | Ativar portal de restauro self-service | 39 |
| 5. | OPERAÇÃO | 41 |
| 5.1 | Instalação do agente de gestão | 41 |
| 5.1.1 | Instalar o Agente Windows | 42 |
| 5.1.2 | Instalar o Agente Linux | 43 |
| 5.1.3 | Instalar Agente MAC | 44 |
| 5.1.4 | Máquinas encontradas e estado dos agentes | 44 |
| 5.2 | Discovery | 45 |
| 5.3 | Instalação do agente de backup | 50 |
| 5.4 | Remoção de agentes | 53 |
| 5.5 | Configurar um backup job | 55 |
| 5.6 | Criação/edição de políticas de backup | 58 |
| 5.7 | Gestão de backup jobs | 67 |
| 5.8 | Recuperação granular de ficheiros via portal | 70 |
| 5.9 | Recuperação completa da máquina | 75 |
| 5.9.1 | Criação do meio de recuperação em máquinas Windows | 75 |
| 5.9.2 | Criação do meio de recuperação em máquinas Linux | 79 |
| 5.9.3 | Recuperação com base no Recovery Media Windows | 79 |
| 5.9.4 | Recuperação com base no Recovery Media Linux | 87 |
| 5.10 | Recuperação de itens aplicacionais | 95 |

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.

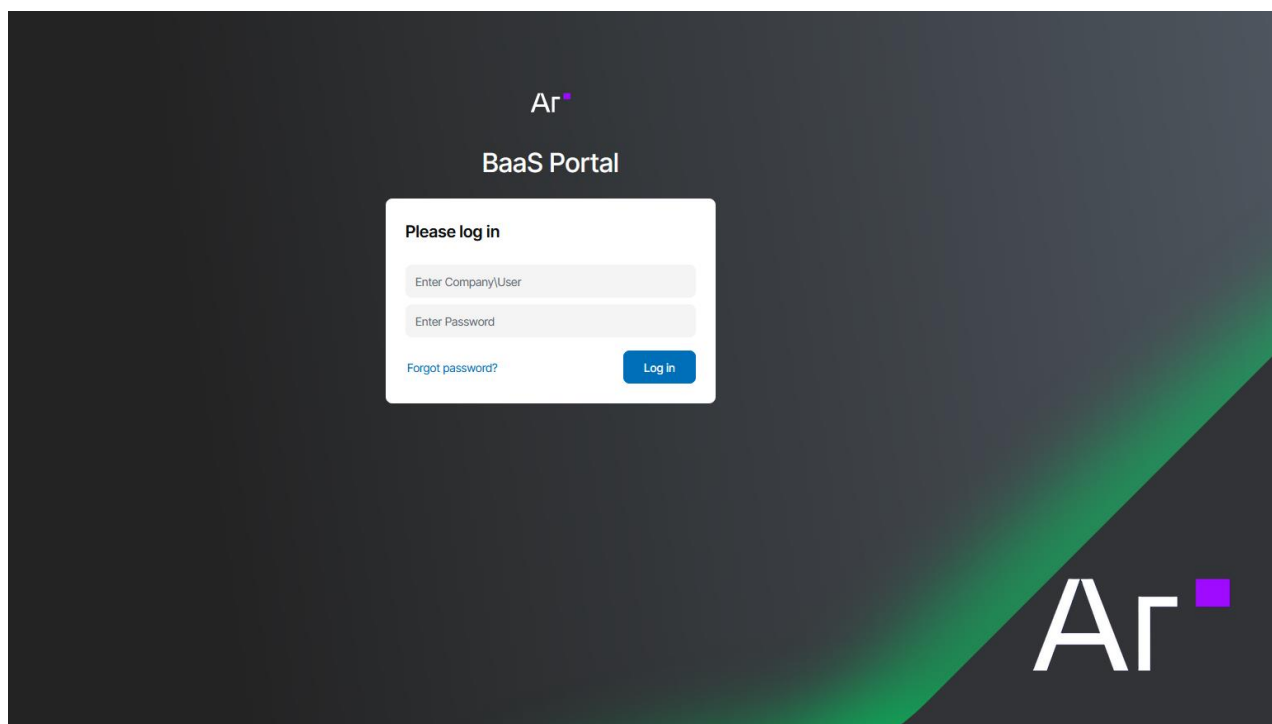
Esta versão do documento é dirigida a parceiros ("Resellers") e inclui funcionalidades acrescidas face à versão para clientes finais.

Qualquer uma das versões 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.

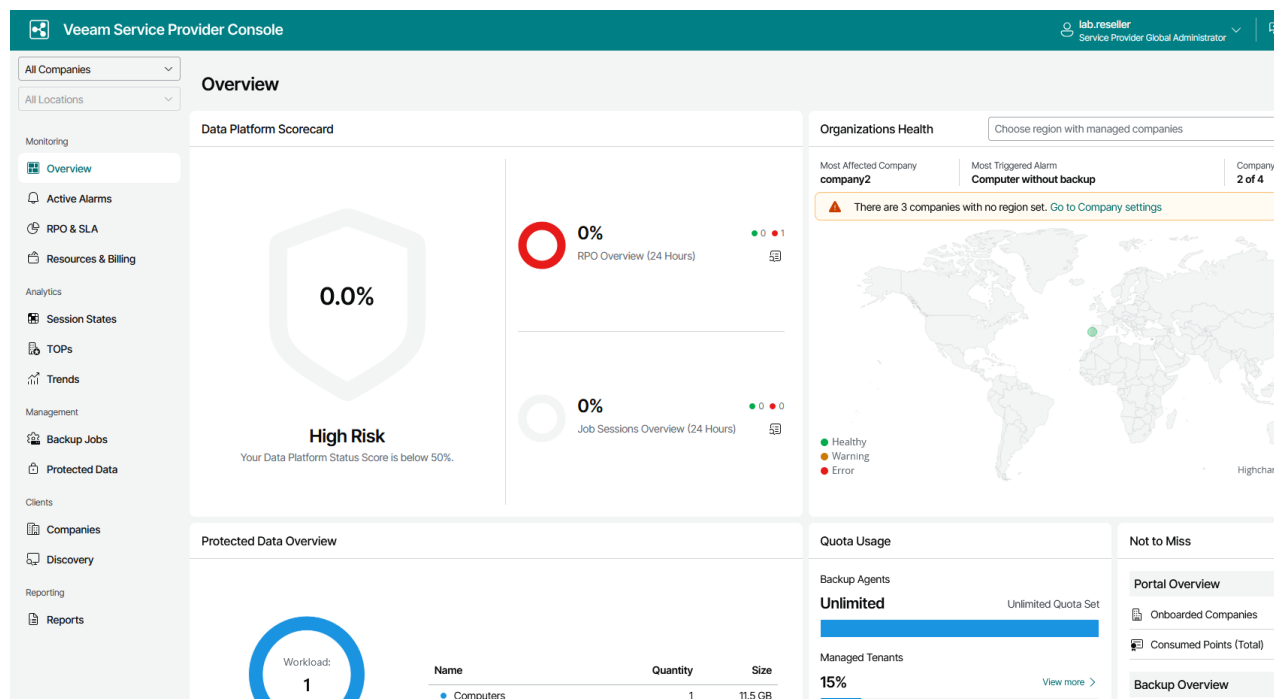
Para aceder, introduzir o utilizador e password enviados pela Ar, no formato **Reseller Name\User**.

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. CONFIGURAÇÃO DE RESELLER

Ao entrar no portal, será mostrada a página "Overview" onde pode ver informações várias sobre o estado e configurações dos serviços.

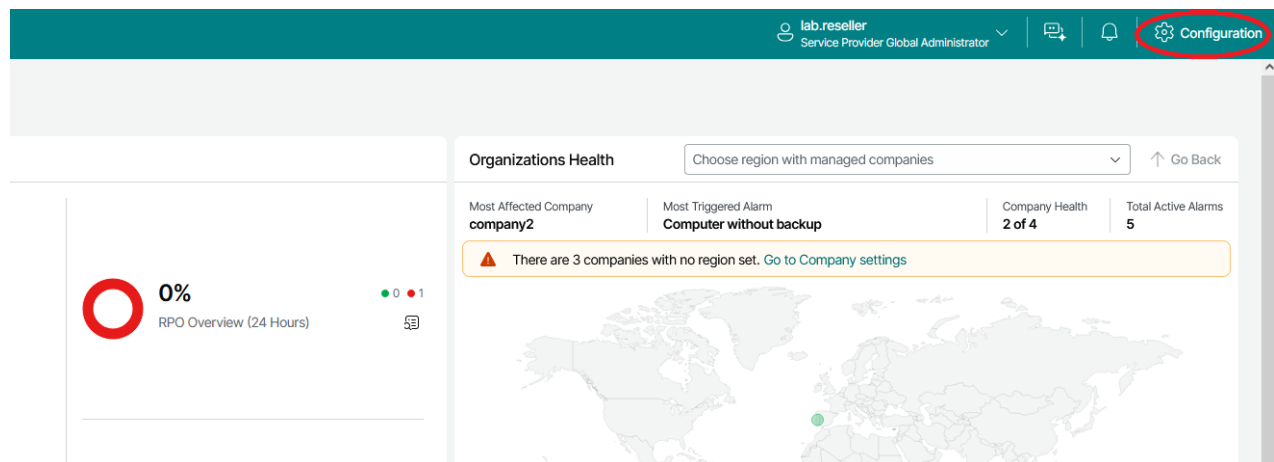
No modo Reseller, o portal para o revendedor encontra-se não formatado, ou seja, sem qualquer modificação de marca.

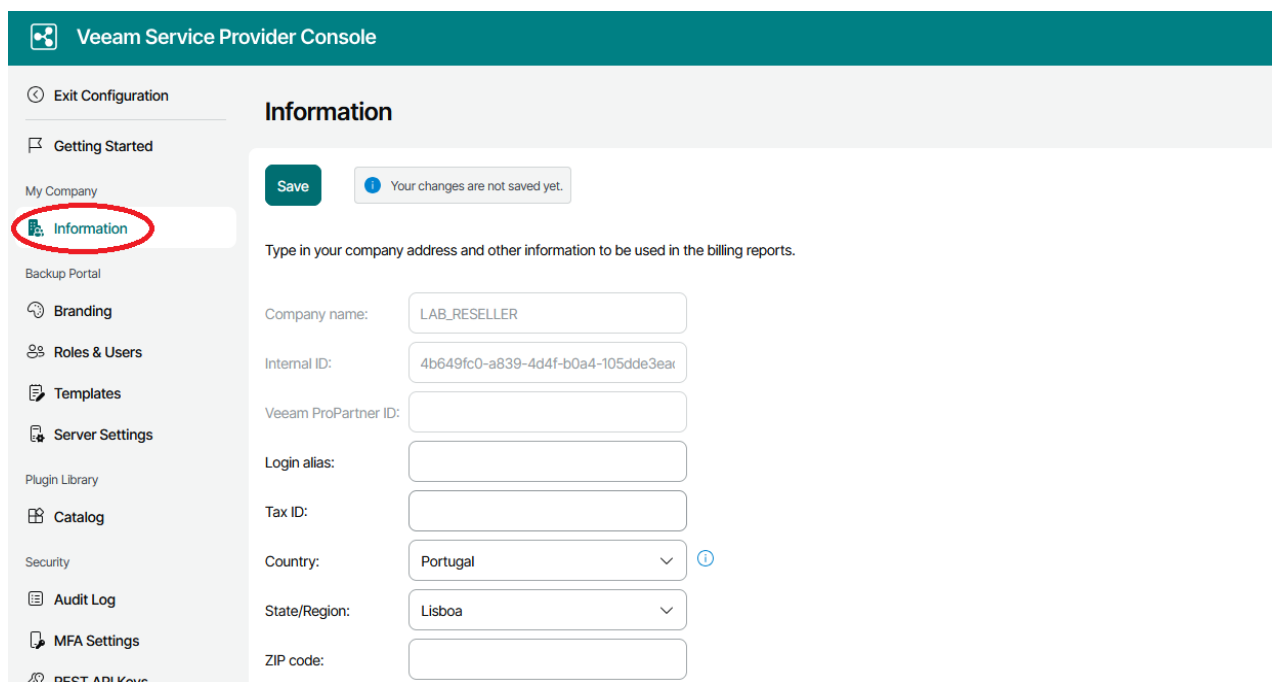


3.1 Perfil do reseller

O primeiro passo é fazer a configuração do Reseller.

Para isso, deverá carregar em "Configuration" no canto superior direito, seguido de "Information" no menu lateral esquerdo.



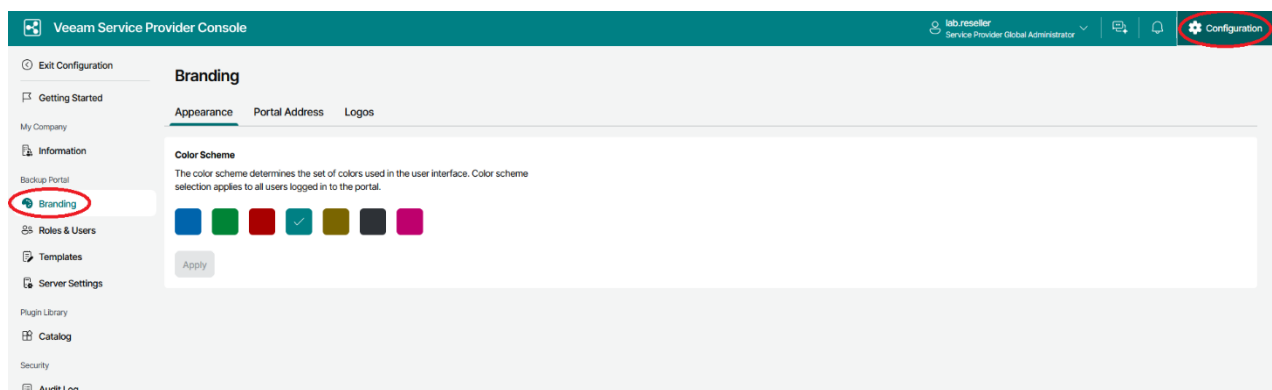


Neste formulário poderá preencher dados específicos da sua organização.

3.2 Branding

O portal permite aos parceiros (Resellers) a modificação do branding. Caso não o façam, o portal será apresentado com a configuração default Veeam e não com o branding Ar.

Para isso, deverá ir a "Configuration" no canto superior direito, seguido de "Branding" no menu lateral esquerdo.



Aqui poderá alterar as características do portal:

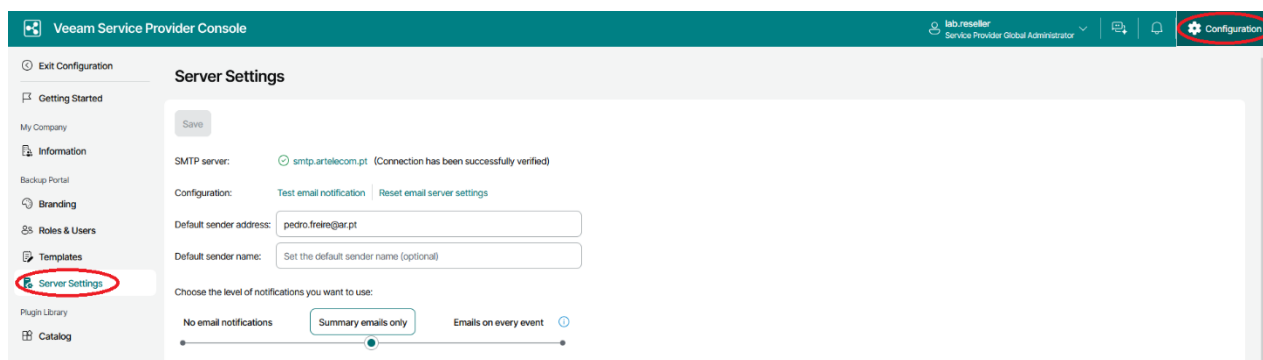
- Esquema de cores
- Endereço web do Portal: FQDN incluindo a porta (exemplo: <https://reseller1.dpconsole.artelecom.pt:1280>)
- Nome do Portal
- Logo da página de Login (a imagem deve ser no formato PNG sem transparência com as dimensões máximas de 48x48 pixels)

- Gráfico da página de Login (a imagem deve ser no formato PNG sem transparência com as dimensões máximas de 756x450 pixels)
- Logo do Portal (a imagem deve ser no formato PNG sem transparência com as dimensões máximas de 400x32 pixels)
- Logo dos Relatórios (a imagem deve ser no formato PNG sem transparência com as dimensões máximas de 200x45 pixels)
- Ícone do Web site (a imagem deve ser no formato ICO com as dimensões 16x16 pixels)

3.3 Notificações

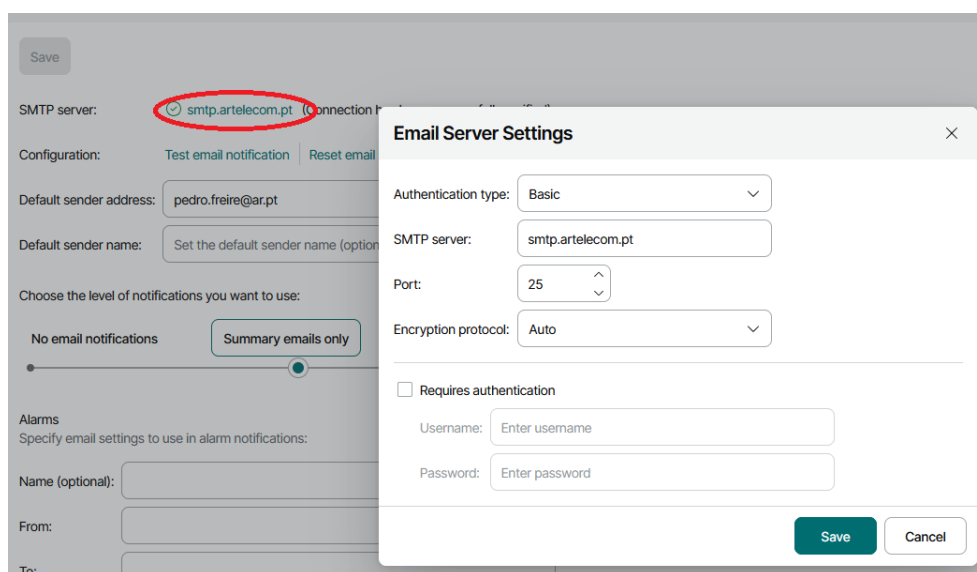
Para receber notificações por email, é necessário primeiro configurar um servidor SMTP.

Para isso, deverá ir a "Configuration" no canto superior direito, seguido de "Server Settings" no menu lateral esquerdo.



Neste formulário é possível configurar o servidor SMTP e vários outros parâmetros, incluindo o nível de notificações pretendido.

Aqui surge a indicação de SMTP server "Not set yet..." ou o endereço do servidor caso tenha sido configurado previamente. Em qualquer dos casos, carregando em cima, é possível (re)configurar em conformidade:



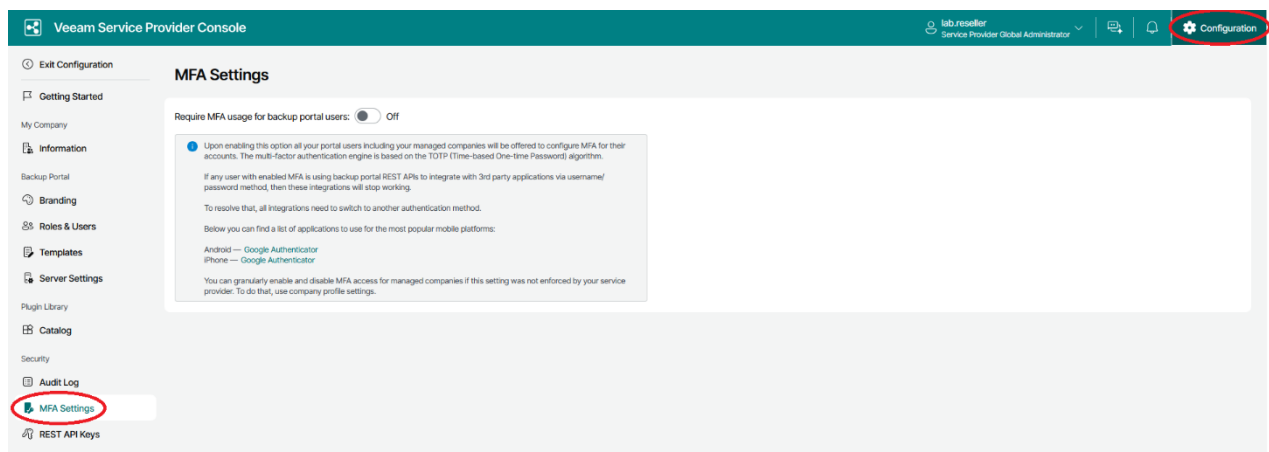
3.4 Autenticação Multi-Factor (MFA)

Para segurança adicional, pode configurar a autenticação multi-factor para o acesso ao portal.

O método é baseado no algoritmo TOTP e implica a instalação de uma aplicação num dispositivo confiável, por exemplo, smartphone. Todas as aplicações que usem o mecanismo TOTP são suportadas, no entanto, recomenda-se o **Google Authenticator**.

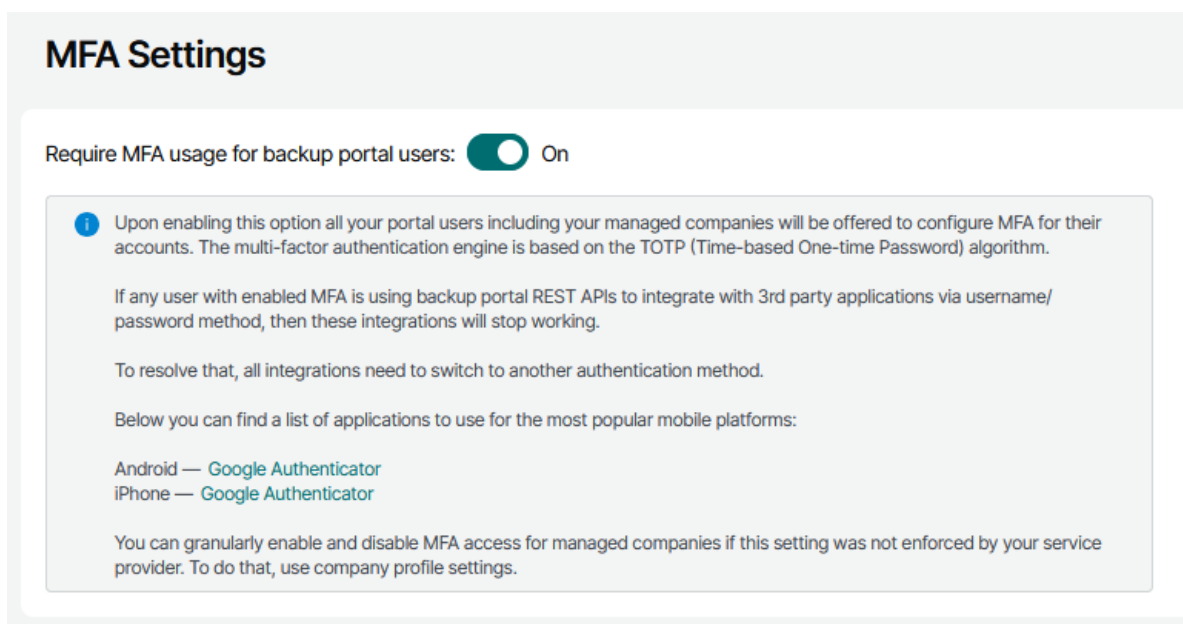
A sua utilização pode ser forçada para todos os utilizadores ou pode ser configurada caso a caso. No caso de não ser forçada, a MFA pode ser configurada pelo próprio utilizador ou pelos administradores.

Para aceder à configuração, deverá ir a "Configuration" no canto superior direito, seguido de "MFA Settings" no menu lateral esquerdo.

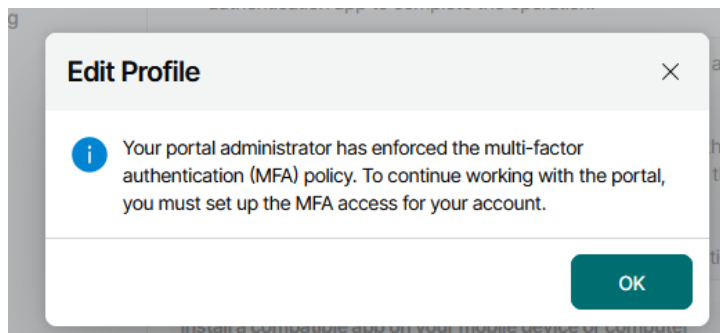


Forçar a utilização para todos os utilizadores

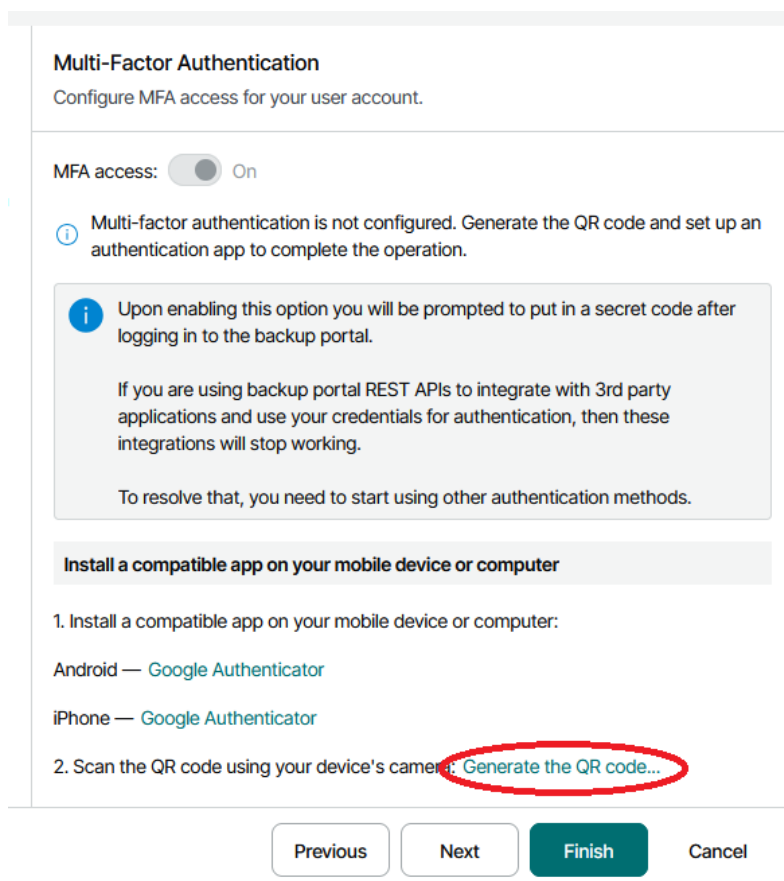
Esta funcionalidade só pode ser ativada pelos administradores.



Ao utilizador que ainda não tenha a MFA configurada será pedido para o fazer aquando do login:

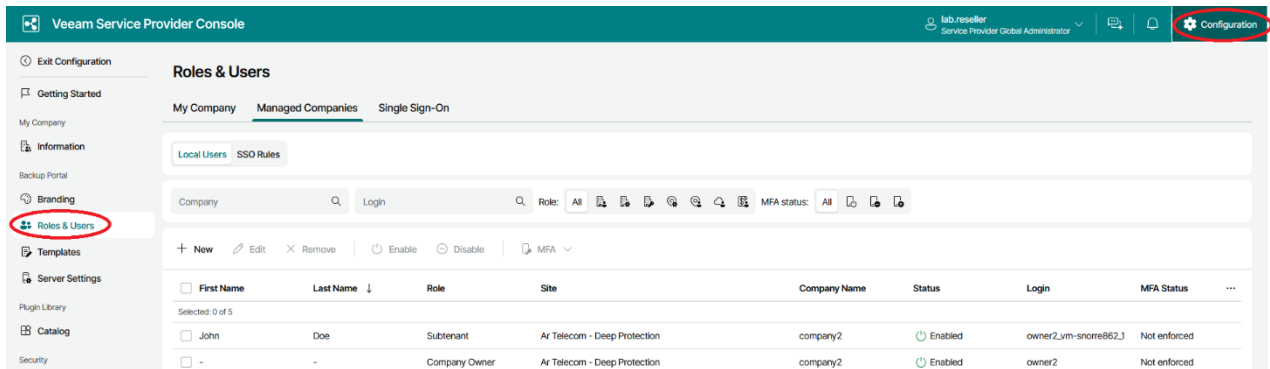


Neste quadro deverá ativar a autenticação multi-factor, instalar a aplicação para a plataforma pretendida e configurar através do scan do código QR.

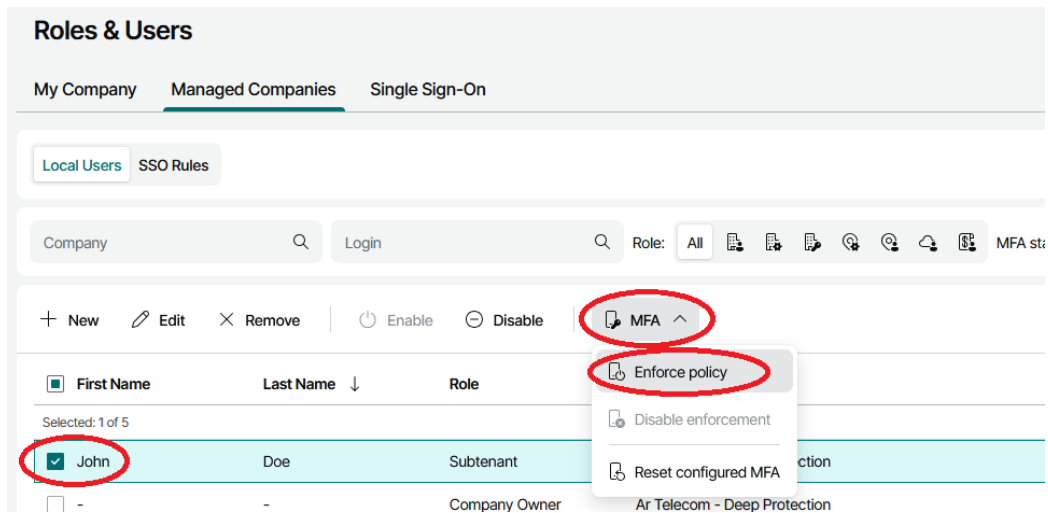


Ativação de MFA em utilizadores específicos – configurado por administradores

Ir a "Configuration" no canto superior direito seguido de "Roles & Users" no menu lateral esquerdo

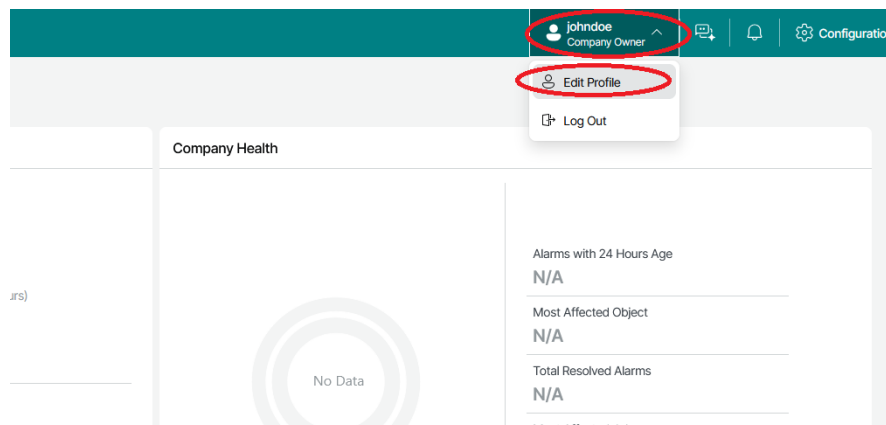


Selecionar a opção pretendida: "My Company" (reseller) ou "Managed Companies" (organizações geridas pelo reseller), selecionar os utilizador(es) pretendido(s) e forçar MFA:



Ativação de MFA configurada pelo próprio utilizador

Após o utilizador fazer login, deverá ir ao ícone de utilizador e carregar em "Edit Profile".



De seguida, carregar em "Multi-Factor Authentication" no menu lateral esquerdo.

Edit Profile

User Info
 Login Info
 Multi-Factor Authentication
 Portal Branding
 Summary

Multi-Factor Authentication
Configure MFA access for your user account.

MFA access: Off

Upon enabling this option you will be prompted to put in a secret code after logging in to the backup portal.
 If you are using backup portal REST APIs to integrate with 3rd party applications and use your credentials for authentication, then these integrations will stop working.
 To resolve that, you need to start using other authentication methods.

Install a compatible app on your mobile device or computer

1. Install a compatible app on your mobile device or computer:

Android — Google Authenticator
iPhone — Google Authenticator

2. Scan the QR code using your device's camera: Generate the QR code...

Previous Next **Finish** Cancel

Neste quadro deverá ativar a autenticação multi-factor, instalar a aplicação para a plataforma pretendida e configurar através do scan do código QR.

3.5 Configuração de tarifários (planos de subscrição)

Os resellers podem criar planos de subscrição, tantos quantos forem necessários, que serão atribuídos a um ou mais das suas empresas clientes ("Companies"). Estes planos não são usados no nosso modelo comercial. Se o pretenderem fazer, devem ir a "Configuration" e em seguida, no menu lateral esquerdo, carregar em "Templates".

Veeam Service Provider Console

lab.reseller Service Provider Global Administrator Configuration

Templates

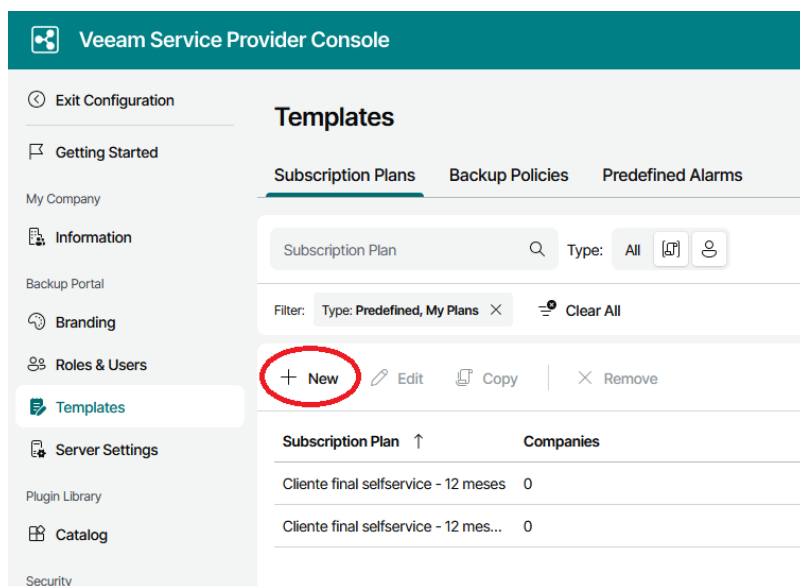
Subscription Plans Backup Policies Predefined Alarms

Subscription Plan

Filter: Type: Predefined, My Plans Clear All

| Subscription Plan | Companies | Currency | Tax | Discount | Created by | Description | ... |
|---------------------------------------|-----------|----------|---------|----------|--------------|-------------|-----|
| Cliente final selfservice - 12 meses | 0 | EUR | VAT 23% | 0% | LAB_RESELLER | - | |
| Cliente final selfservice - 12 mes... | 0 | EUR | VAT 23% | 0% | LAB_RESELLER | - | |

Aqui poderão ver e editar os planos já criados, bem como criar novos planos. É possível copiar um plano existente para um novo plano, não tendo de introduzir todos os dados novamente.



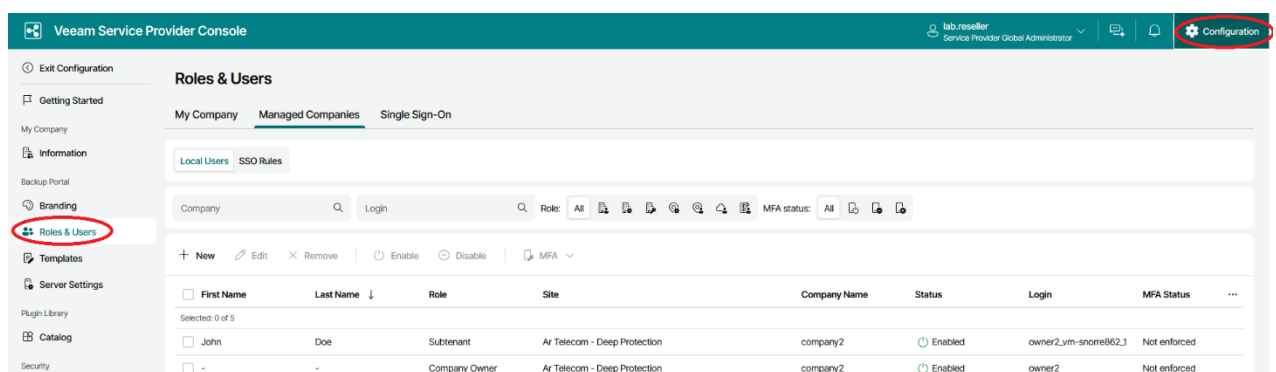
3.6 Gestão de utilizadores do Reseller

Além do utilizador gestor do Reseller (*Global Administrator*), que foi enviado no seu e-mail de Boas Vindas, é possível e desejável criar outros utilizadores com perfis distintos.



Não é possível apagar ou inibir o utilizador gestor (*Global Administrator*) do Reseller criado pela Ar.

Para isso, deverá carregar em "Configuration" no canto superior direito, seguido de "Roles & Users" no menu lateral esquerdo.



Neste quadro tem a opção de gerir os utilizadores próprios do Reseller ("*My Company*") ou das companhias geridas ("*Managed Companies*").

Aqui pode criar, editar, remover, ativar ou inibir utilizadores, assim como definir o estado de autenticação multi factor.

No caso do Reseller, o utilizador pode estar associado a um dos seguintes perfis:

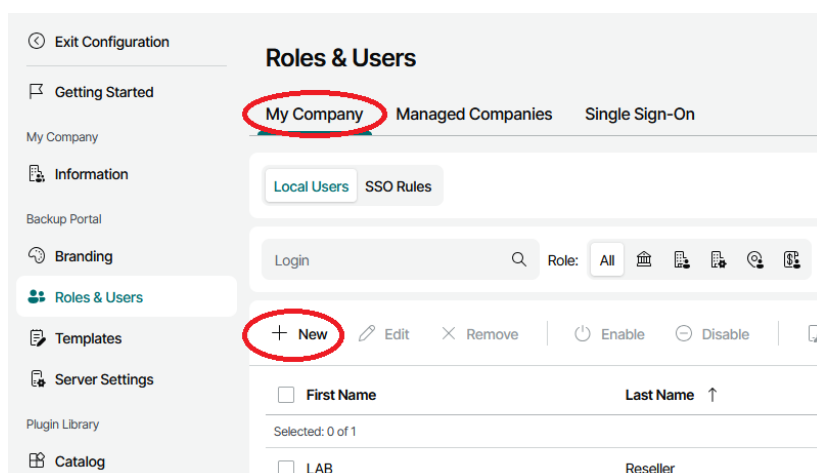
- **Service Provider Global Administrator:** utilizador criado pela Ar aquando da configuração do Reseller. Este utilizador não pode ser alterado nem eliminado.
- **Service Provider Administrator:** este utilizador tem as mesmas permissões que o Global Administrator, mas pode ser eliminado pelo último.
- **Service Provider Operator:** permite gerir a operação e todo o processo de configuração e execução de cópias de segurança e restauros.
- **Service Provider User:** estes utilizadores apenas têm permissão de leitura de informação parcial.
- **Service Provider Invoice Auditor:** este perfil apenas dá acesso ao menu "Invoices" onde pode consultar e processar informação sobre faturação.



É possível modificar o perfil de utilizador mais tarde, bastando para isso editar o utilizador e alterar para o novo perfil pretendido. Não é possível fazê-lo para o utilizador que está com a sessão iniciada.

De seguida apresentam-se as instruções para criar utilizadores locais do próprio Reseller. 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 em <https://www.veeam.com/pt/products/service-provider/console/resources.html>

Para criar um utilizador local do Reseller, carregar em "New" no separador "My Company":



A informação sobre o utilizador é opcional e pode ser deixada em branco, bastando preencher a informação de login:

De seguida escolhe-se 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.

Finalmente a opção de obrigatoriedade de autenticação multi-factor:

< Back | **New Local User**

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

Multi-Factor Authentication
Configure MFA access.

Mandatory MFA usage: Off

i Upon enabling this option user will be asked to configure multi-factor authentication for the backup portal.

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

< Back | **New Local User**

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

Summary
Review user details and click Finish to exit the wizard.

User Info

First name:
Last name:
Email address:
Username: user1

Role

Role: Service Provider Administrator

Multi-Factor Authentication

MFA status: Not enforced

Previous **Finish** Cancel

4. GESTÃO DE COMPANHIAS PELO RESELLER

Na consola Veeam Service Provider Console (VSPC), um cliente de um reseller denomina-se **Company**. Uma companhia é uma organização que consome recursos respeitantes a um reseller.

Para aceder à gestão de companhias, ir a “Companies” no menu lateral esquerdo do quadro principal da consola. Aqui poderá verificar o estado das companhias e efetuar ações sobre as mesmas:

- Criar
- Editar
- Remover
- Ativar ou desativar
- Gerir Localizações e Utilizadores
- Associar um plano de subscrição
- Reiniciar o token de segurança
- Reenviar o email de Boas Vindas
- Forçar ou ignorar o uso de autenticação multi-fator

Inicialmente não existem companhias criadas, pelo que, será necessário criar uma.

4.1 Criar companhia

The screenshot shows the 'Companies' management page in Ar Cloud. On the left is a sidebar with navigation options. The main area has a search bar and a filter for 'MFA status' set to 'All'. Below that is a toolbar with a '+ New' button circled in red, along with 'Edit', 'Remove', 'Enable', 'Disable', and 'Manage' buttons. A table header is visible with columns for 'Company', 'MFA Status', 'Administrators', 'Portal Users', and 'State'. The table content is currently empty, showing 'No data to display'.

O processo de criação de uma companhia é semelhante ao da configuração do perfil do reseller, só que neste caso:

- é necessário indicar o "Company name";
- apesar de ser opcional, deve também preencher os dados de um contacto dessa companhia (o endereço de email aqui configurado será considerado o Company Owner e será usado para enviar notificações como o welcome email e alarmes);
- Company ID é opcional e poderá servir para identificar a companhia com um código específico do reseller;
- Veeam Tenant ID será obtido automaticamente após configuração do mapeamento com VCSP Pulse (opcional)

< Back | **New Company**

- Company Info**
- User Info
- Services
- Billing
- Multi-Factor Authentication
- Notifications
- Summary

Company Info
Specify company name and contact information.

Company name: MyFirstCompany1

Login alias:

Tax ID:

Title:

First name: user1

Last name:

Email address: user1@myfirstcompany1.com

Telephone:

Country: ⓘ

State/Region:

Company ID:

Veeam Tenant ID:

ZIP code:

Website:

Previous Next Cancel

4.1.1 User Info

Neste quadro introduzem-se os detalhes do utilizador do portal para esta companhia.

< Back | **New Company**

- Company Info
- User Info**
- Services
- Billing
- Multi-Factor Authentication
- Notifications
- Summary

User Info
Create the backup portal user account.

Username: user1

Password: ●●●●●●●●●● ⓘ

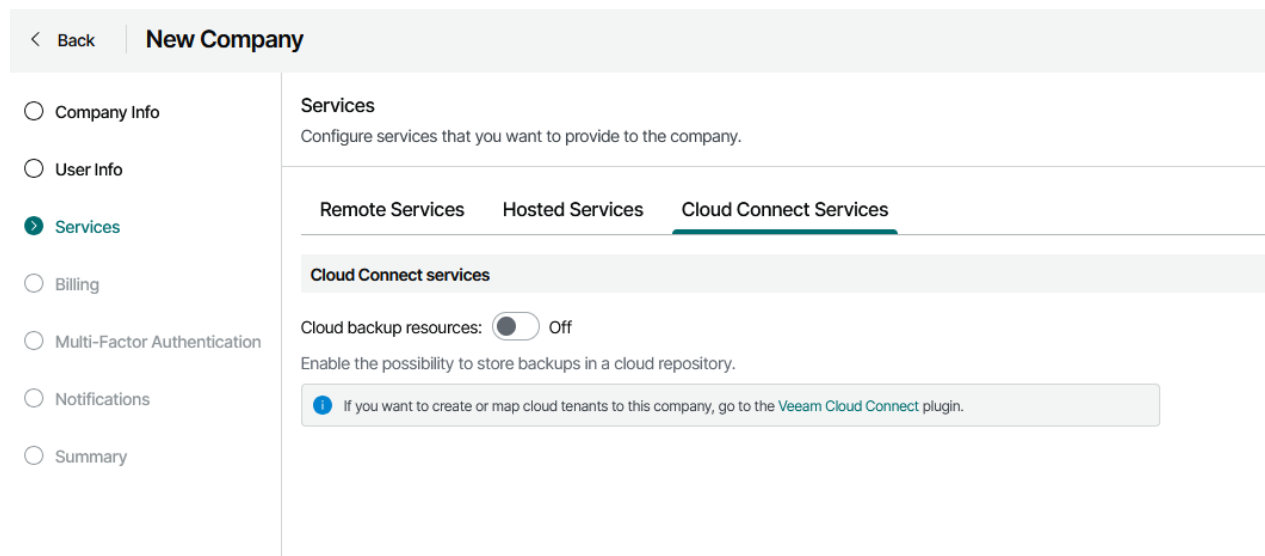
Confirm password: ●●●●●●●●●● ⓘ

! The specified credentials apply to the Company Owner user account in the Veeam Service Provider Console only. They are not linked to the Veeam Cloud Connect tenant account. Tenant accounts should be configured separately in the [Veeam Cloud Connect plugin](#).

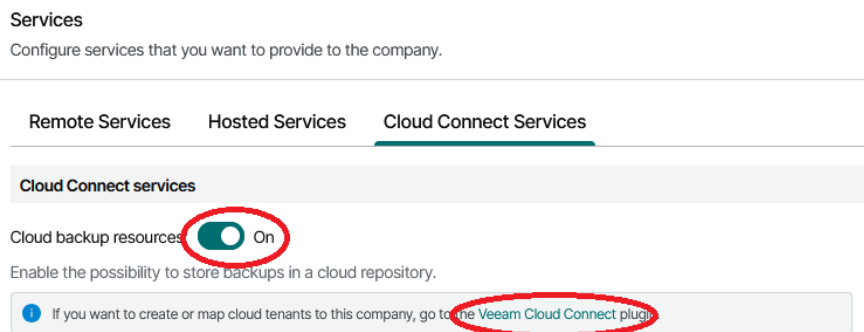
4.1.2 Configuração de serviços associados à companhia

O passo seguinte será configurar os serviços associados a esta companhia.

Existem três tipos de serviços que podem ser configurados aqui mas a opção a escolher deverá ser **Cloud Connect Services**



A configuração dos serviços Cloud Connect é efetuada no quadro de configuração do plugin (em <https://dpconsole.artelecom.pt:1280/plugins/vcc/resources>):



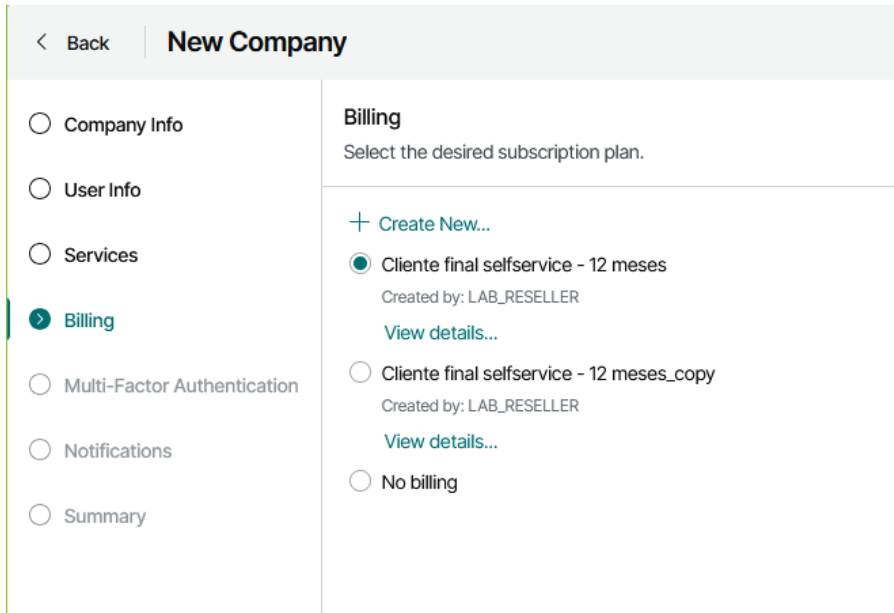
4.1.3 Billing

A consola permite medir os recursos atribuídos e consumidos pelas companhias, calcular os custos desses recursos, e gerar uma fatura para cada companhia.

A lista dos serviços/recursos e os valores encontra-se definida nos **"Subscription Plans"**.

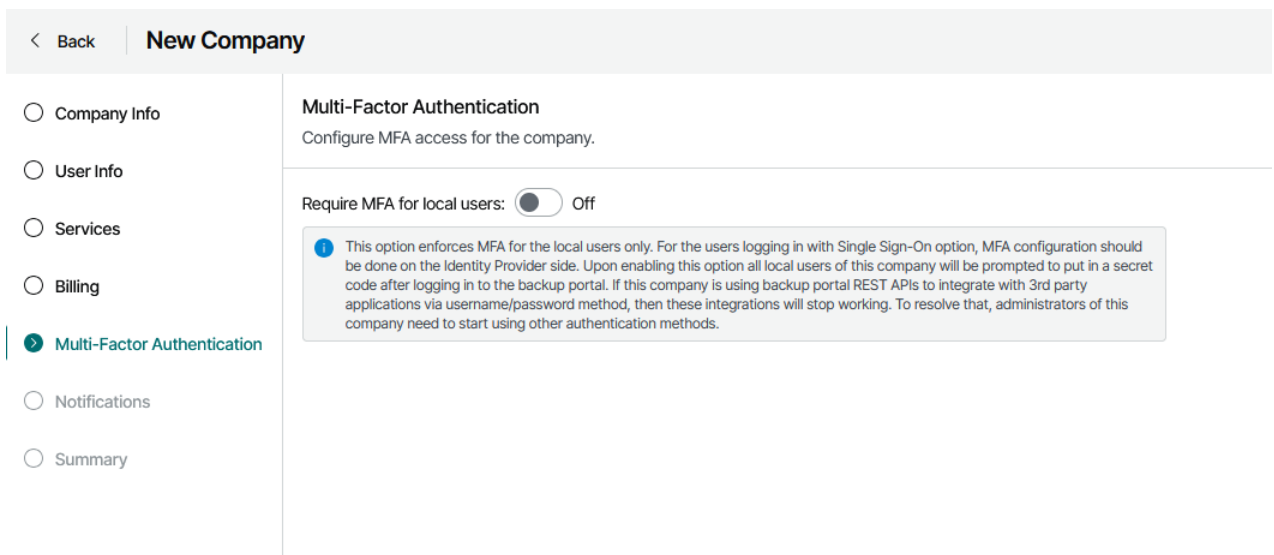
Neste quadro é possível optar por não fazer qualquer tipo de billing, selecionar um plano criado anteriormente ou criar um novo plano. A opção de criar um novo plano leva-nos para o mesmo quadro visto anteriormente na secção de CONFIGURAÇÃO DE RESELLER.

A opção recomendada é **"No billing"**



4.1.4 Multi-Factor Authentication

Permite ativar a autenticação multi-factor para todos os utilizadores. Na próxima sessão de login de cada utilizador será solicitado que configure a MFA.



4.1.5 Notificações

Aqui é possível personalizar o welcome email e os parâmetros de notificações de alarmes.

É possível incluir tanto texto simples como tags HTML na secção de texto do email.

< Back | **New Company**

- Company Info
- User Info
- Services
- Billing
- Multi-Factor Authentication
- Notifications**
- Summary

Notifications
Configure notification settings for the company.

Welcome email

Include custom text: On Off

Specify text to add to the welcome email. It may contain URL: ⓘ

Include Self-Service Portal section in the welcome email

Use this template as default for all managed companies

[Preview welcome email...](#)

Predefined alarms

Company alarms: On Off

ⓘ Upon enabling this option, all alarms in the client's backup portal will be enabled by default. This option is recommended when managed companies have their own technicians monitoring backup job states.

Ao ativar "Enable company alarms" esta companhia terá o seu próprio conjunto de alarmes e os utilizadores do portal poderão verificar os mesmos no portal.

Finalmente, na secção "Summary" poderá rever as configurações e ativar a Companhia.

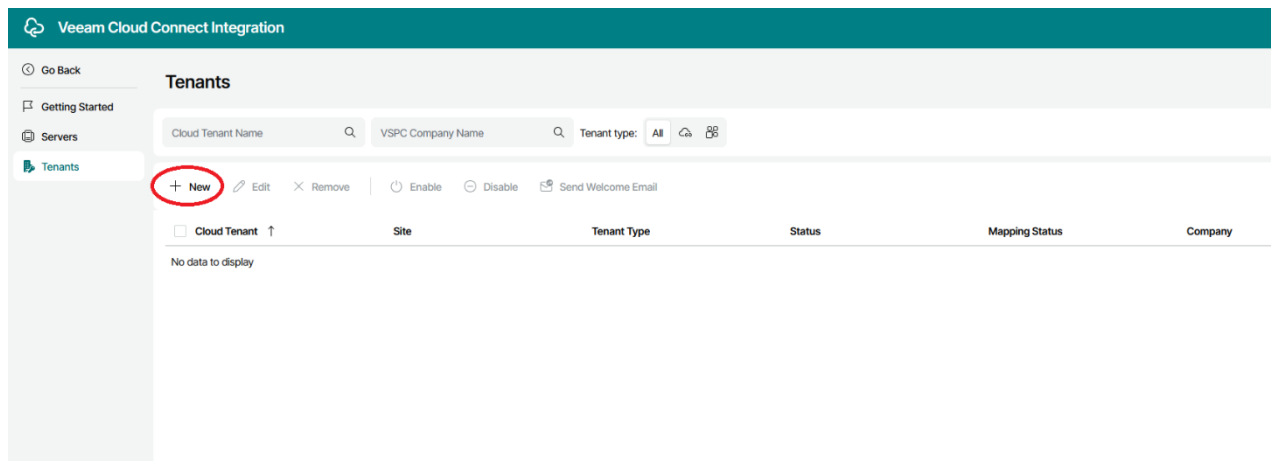
As credenciais a usar para aceder à consola VSPC serão no formato `<CompanyName>\<Username>`

4.2 Criação e gestão de Tenants

Conforme mensagem no quadro 4.1.1 (User Info), para que esta companhia tenha acesso aos repositórios contratados à Ar, é necessário configurar o utilizador no plugin **Cloud Connect**, com as credenciais enviadas no email de boas vindas enviado pela Ar.

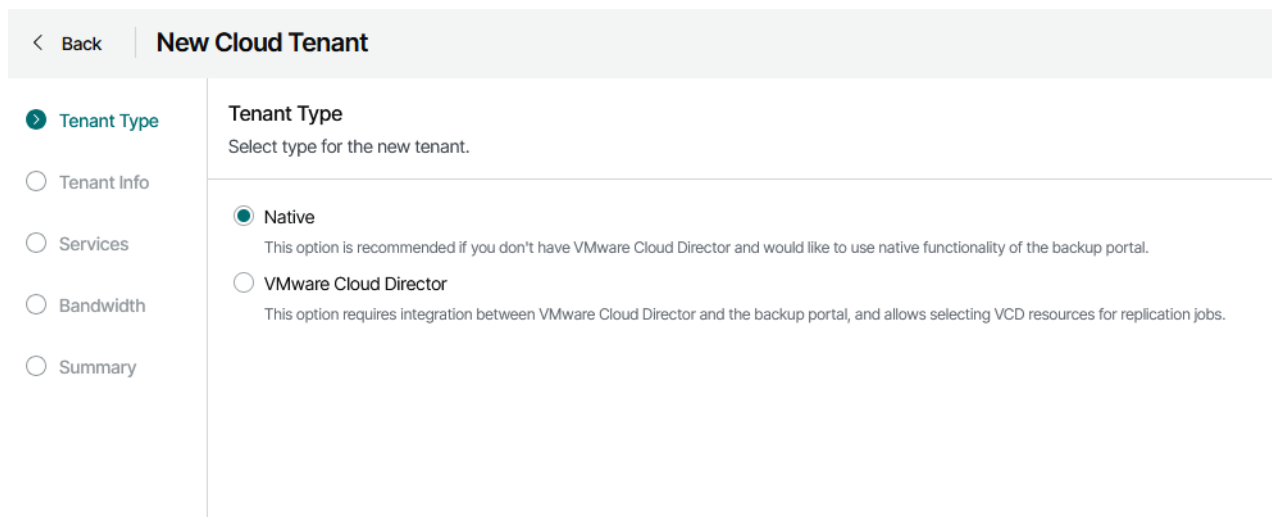
A configuração do tenant para os serviços Cloud Connect é efetuada no quadro de configuração do plugin (em <https://dpconsole.artelecom.pt:1280/plugins/vcc/resources>):

Fazendo New:



Surge um quadro para criar o tenant, onde se começa por dizer qual o tipo de tenant.

A opção a escolher deve ser do tipo **Native**



O quadro que surge agora permite criar um novo tenant Cloud Connect e associá-lo à companhia criada.

O "Site" a escolher é o que foi atribuído ao reseller pela Ar: **Ar – Deep Protection** e deve ser criado um utilizador e password para gerir o acesso a este tenant:

< Back **New Cloud Tenant**

- Tenant Type
- Tenant Info**
- Services
- Bandwidth
- Summary

Tenant Info
Create a tenant account on the selected site.

Site: Ar Telecom - Deep Protection

Username: myuser1

Password: ●●●●●

Confirm password: ●●●●●

Disable account automatically on 5/8/2026

Description:
Created by LAB_RESELLER in Veeam Service Provider Console at 5/8/2026 5:21 PM

Company mapping

Map the created tenant to a Veeam Service Provider Console company.

Company: MyFirstCompany1 (managed by: LAB_RESELLER)

Previous **Next** Cancel

4.2.1 Serviços

Backup resources

Permite o acesso a repositórios de backup na Ar. É necessário configurar os repositórios que irão estar disponíveis a esta companhia. Fazendo **Next** no quadro anterior, passamos ao próximo quadro, onde se ativa o acesso aos recursos de backup (repositórios), bastando para isso ativar a opção e configurar o(s) resositório(s):

< Back | **New Cloud Tenant**

- Tenant Type
- Tenant Info
- Services**
- Bandwidth
- Summary

Services
Configure Cloud Connect services that you want to provide to the tenant.

Backup resources: On
Enable the possibility to store backups in a cloud repository.

Backup repository [Configure...](#)

Replication resources: Off
Enable the possibility to replicate VMs to a cloud host.

Carregando em **Configure:**

Backup Resources
Select one or more backup repositories and assign cloud storage quota.

+ Add Edit Set As Default Remove

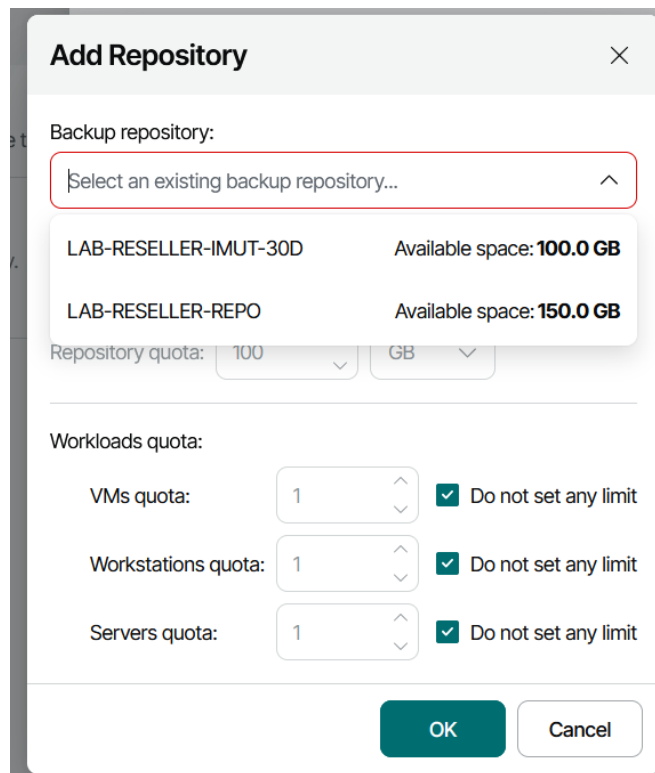
| Backup Repository | Cloud Repository | Quota | Default Repository | WAN Accelerator |
|--------------------|------------------|-------|--------------------|-----------------|
| No data to display | | | | |

Protect deleted backup files for days

Option to protect deleted backup files is not available for object storage repositories.

Apply Cancel

e depois em **Add:**



Permite seleccionar o repositório pretendido e atribuído ao reseller, dar um nome ao repositório para este tenant e definir quotas, quer de espaço no repositório, quer de licenças de dispositivos a salvaguardar.

As quotas de VMs, Workstations e Servers, não impõem qualquer restrição física e serve apenas como valor de limiar que ao ser atingido gera um alarme *VMs stored in cloud repository*, *Workstation agent backups stored in cloud repository* ou *Server agente backups stored in cloud repository*. Estes alarmes podem ser customizados de acordo com o pretendido.

4.2.2 Bandwidth

Nesta etapa da configuração, é possível especificar limitações de tarefa e largura de banda para as tarefas do Veeam Backup & Replication que utilizam recursos remotos. Limitar a largura de banda entre a Companhia e a Ar e o processamento paralelo de tarefas ajuda a evitar a sobrecarga dos gateways, proxies de backup, repositórios de backup e equipamentos de rede no lado do provedor de serviços.

< Back | **New Cloud Tenant**

- Tenant Type
- Tenant Info
- Services
- Bandwidth**
- Summary

Bandwidth
Specify maximum number of task slots available to this company and, if required, limit the incoming network traffic.

Concurrent tasks

Max concurrent tasks:

Each task slot allows processing of a single disk, so companies with one slot assigned will not be able to leverage parallel processing or run multiple jobs concurrently. This setting applies to direct mode transfers only (WAN accelerators process disks sequentially).

Limit incoming network traffic to:

Defines maximum incoming network traffic bandwidth that will be accepted from the tenant. Traffic from tenants with more bandwidth will be throttled to the specified amount.

Gateway pool

Enabled option: Automatic selection [Choose...](#)

Data transfer out

Quota: Off

Set data transfer out quota for Veeam Cloud Connect.

É também possível especificar a quota de dados que a Companhia pode descarregar dos repositórios da Ar. Esta quota não coloca qualquer restrição, serve apenas para desencadear um alarme.



A secção de configuração **"Data transfer out"** apenas estará disponível se forem configurados recursos de backup e/ou replicação.

4.3 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 – *"Default location"*.

As localizações podem ser geridas pelo reseller, acedendo a *"Companies"* no menu lateral esquerdo seleccionando a companhia pretendida, seguindo de *"Manage"* na barra horizontal, e por fim, 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.

4.4 Gestão de Utilizadores

Ao criar uma 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 pelo próprio Company Owner ou pelos utilizadores do Reseller com perfil Global Administrator, Administrator ou Operator.



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

Os utilizadores podem ser geridos pelo reseller, acedendo a "Companies" no menu lateral esquerdo seleccionando a companhia pretendida, seguindo de "Manage" na barra horizontal, e por fim, escolhendo a opção "Users":

The screenshot shows the 'Companies' management interface. On the left sidebar, the 'Companies' menu item is highlighted with a red circle. The main content area displays a table of companies with columns for 'Company', 'MFA Status', 'Administrators', 'Portal Users', and 'State'. A dropdown menu is open under the 'Manage' button, showing options: 'Locations', 'Users', 'Set Billing', 'Reset Security Token', and 'Send Welcome Email'.

Alternativamente, pode aceder carregando em "Configuration" no canto superior direito, seguido de "Roles & Users" no menu lateral esquerdo e escolher o separador "Managed Companies".

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.



Contrariamente aos utilizadores do reseller, 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 "Managed Companies":

| First Name | Last Name | Role | Site | Company Name | Status | Lo |
|------------|-----------|----------------|---------------------------|-----------------|---------|----|
| user1 | - | Company Owner | Ar Telecom - Deep Prot... | MyFirstCompany1 | Enabled | us |
| - | - | Company Tenant | Ar Telecom - Deep Prot... | MyFirstCompany1 | Enabled | my |

De seguida, escolhe-se a companhia onde se quer adicionar o utilizador e carrega-se em "Next"

< Back | **New User**

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

Company
Select company that will be assigned to the user.

MyFirstCompany1 X

Filter: Company Name: MyFirstCompany1 X Clear All

| Company | Site |
|-----------------|------------------------------|
| MyFirstCompany1 | Ar Telecom - Deep Protection |

Previous **Next** Cancel

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.

< Back | **New User**

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

Role
Specify a role to assign to the user.

Role: Company Administrator v

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.

< Back | **New User**

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

Role
Specify a role to assign to the user.

Role:

- Company Administrator**
ing, reporting, and billing data and can perform all types of management actions. This role count.
- Location Administrator
ssions for each user role.
- Location User
- Company Invoice Auditor
- Subtenant

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

< Back | **New User**

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

User Info
Enter username and contact information.

Title:

First name:

Last name:

Email address:

< Back | **New User**

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

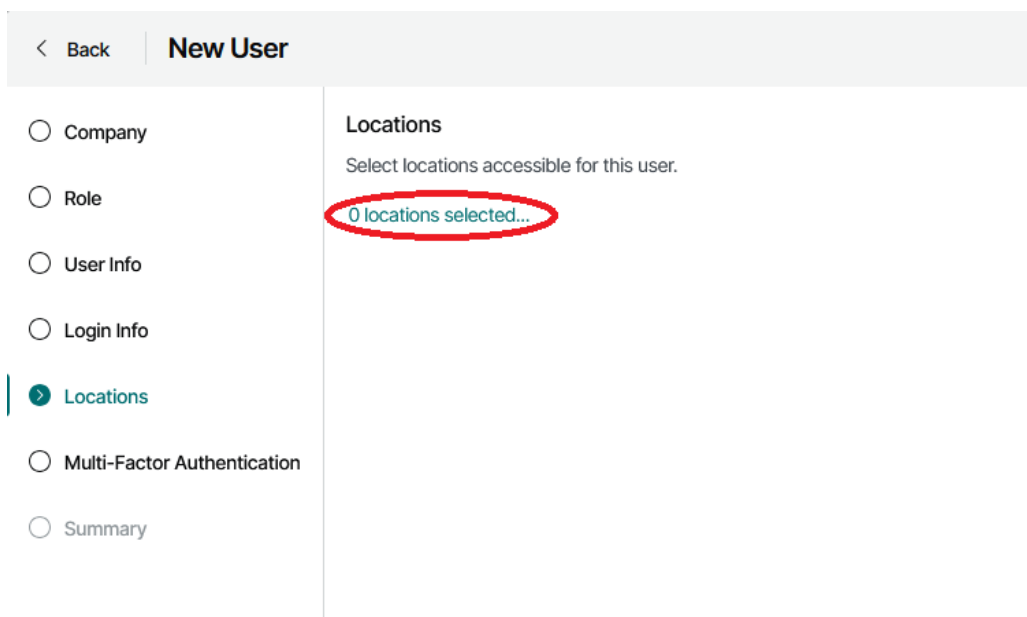
Login Info
Specify login and password for the user.

Login:

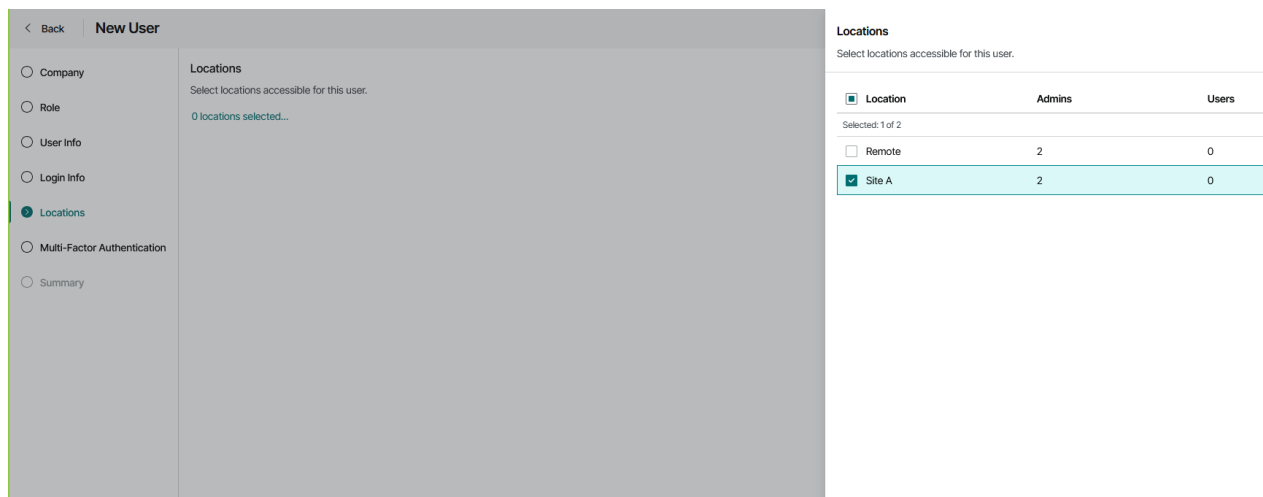
Password:

Confirm password:

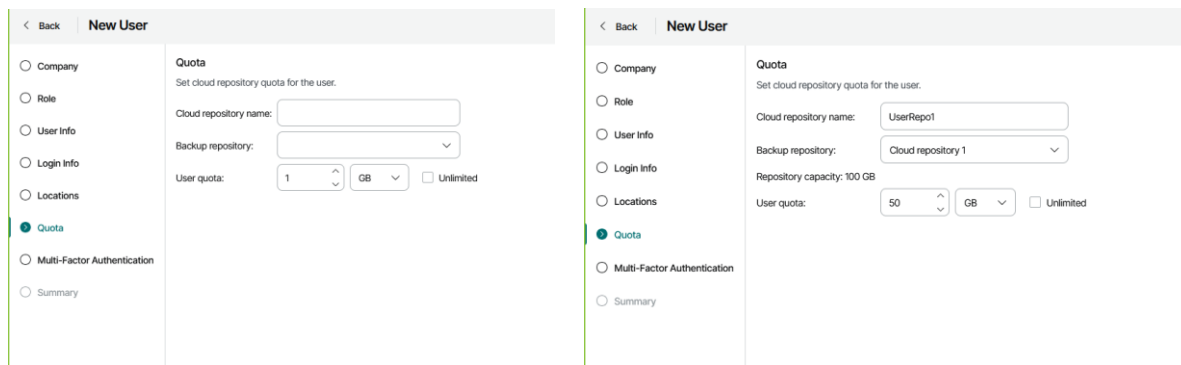
No caso do utilizador a criar ter perfil *Location Administrator*, *Location User* ou *Subtenant* é necessário configurar quais as localizações da companhia a que tem acesso. Assim sendo, é necessário selecionar as localizações no próximo quadro, carregando na seleção de localizações, selecionar as pretendidas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



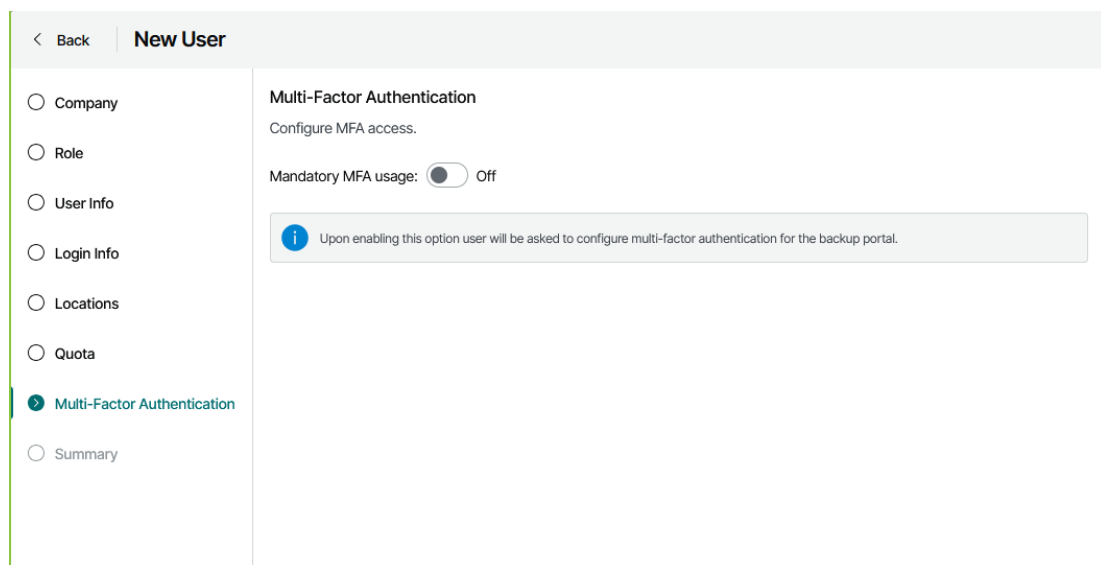
As companhias são criadas sem especificar localizações, pelo que, a única disponível será a "Default location". Depois de configuradas novas localizações, as mesmas estarão disponíveis para seleção neste quadro.



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 o 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.

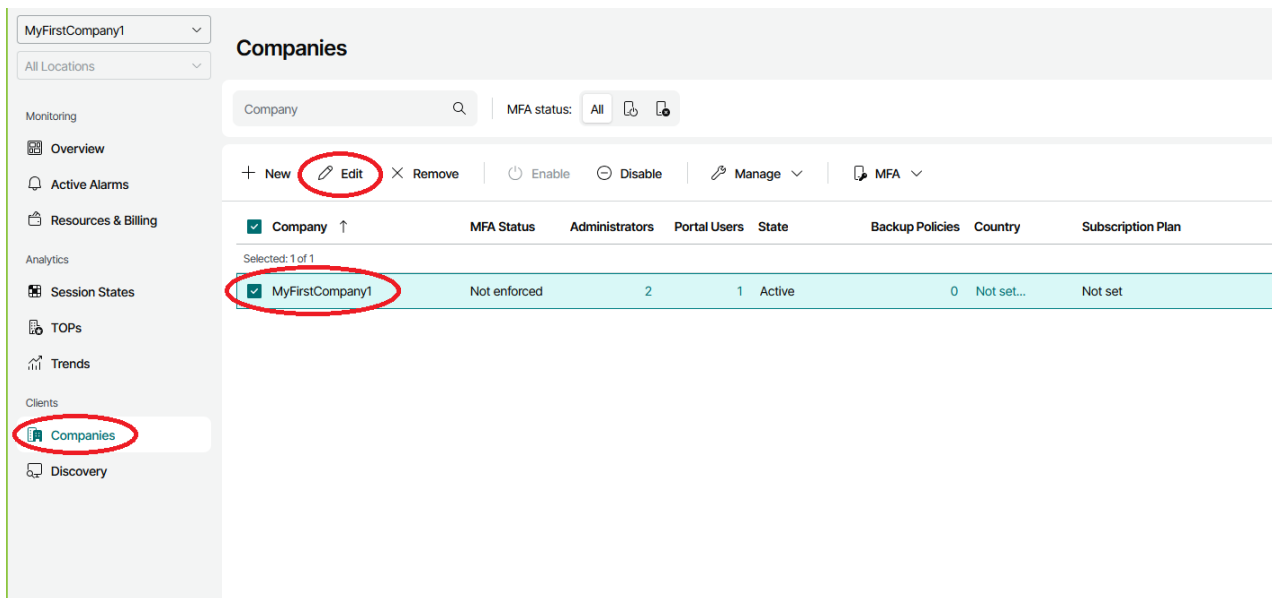


O último passo é rever os dados inseridos e finalizar a criação do utilizador.

4.5 Gestão de Serviços

Os serviços associados às companhias podem ser configurados aquando da criação da companhia ou posteriormente editando a mesma.

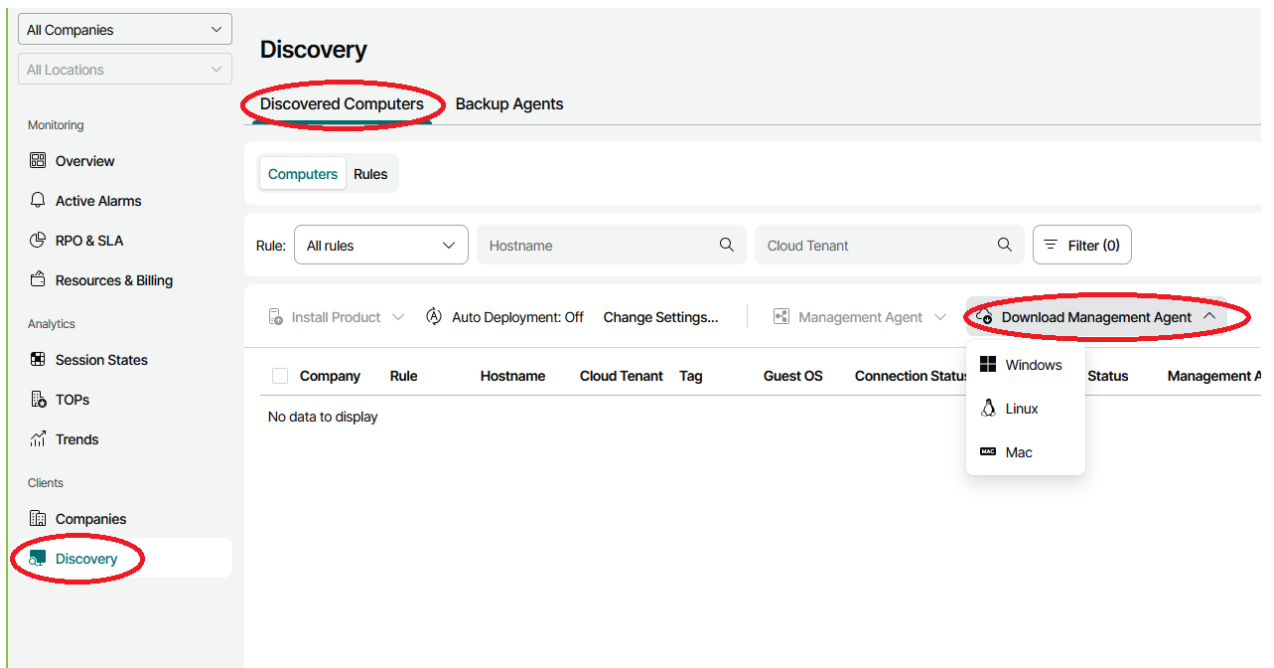
Para o fazer posteriormente, deverá ir a "Companies" no menu lateral esquerdo do quadro principal da consola, escolher a companhia que se quer alterar e carregar em "Edit".



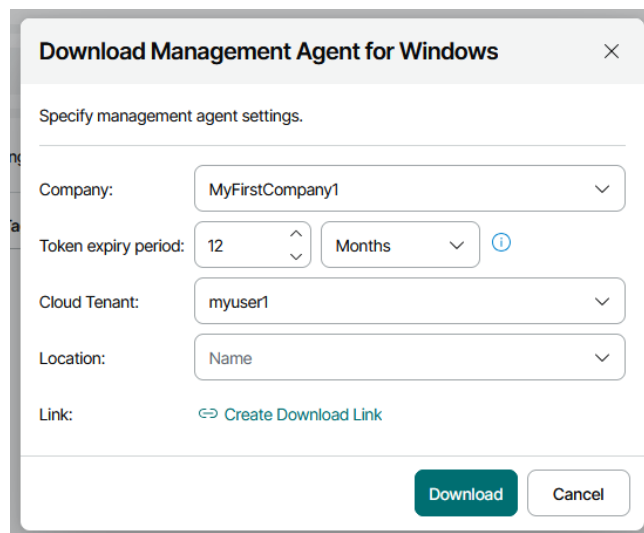
O quadro apresentado é o mesmo de quando se está a criar a companhia, pelo que, deve seguir os passos indicados no ponto [4.1 Criar companhia](#).

4.6 Agente de Gestão

É possível um reseller descarregar e instalar o agente de gestão nas máquinas da companhia pretendida. Para isso, deverá aceder a "Discovery" no menu lateral esquerdo, separador "Discovered Computers" na barra horizontal, seguido de "Download Management Agent", e escolher a plataforma destino pretendida:



Todo o processo daqui para a frente é igual ao caso de ser o administrador da companhia descrito no ponto [5.3 Instalação do agente de gestão](#), excepto que para descarregar o agente é necessário indicar para que companhia se destina.



Download Management Agent for Windows

Specify management agent settings.

Company: MyFirstCompany1

Token expiry period: 12 Months

Cloud Tenant: myuser1

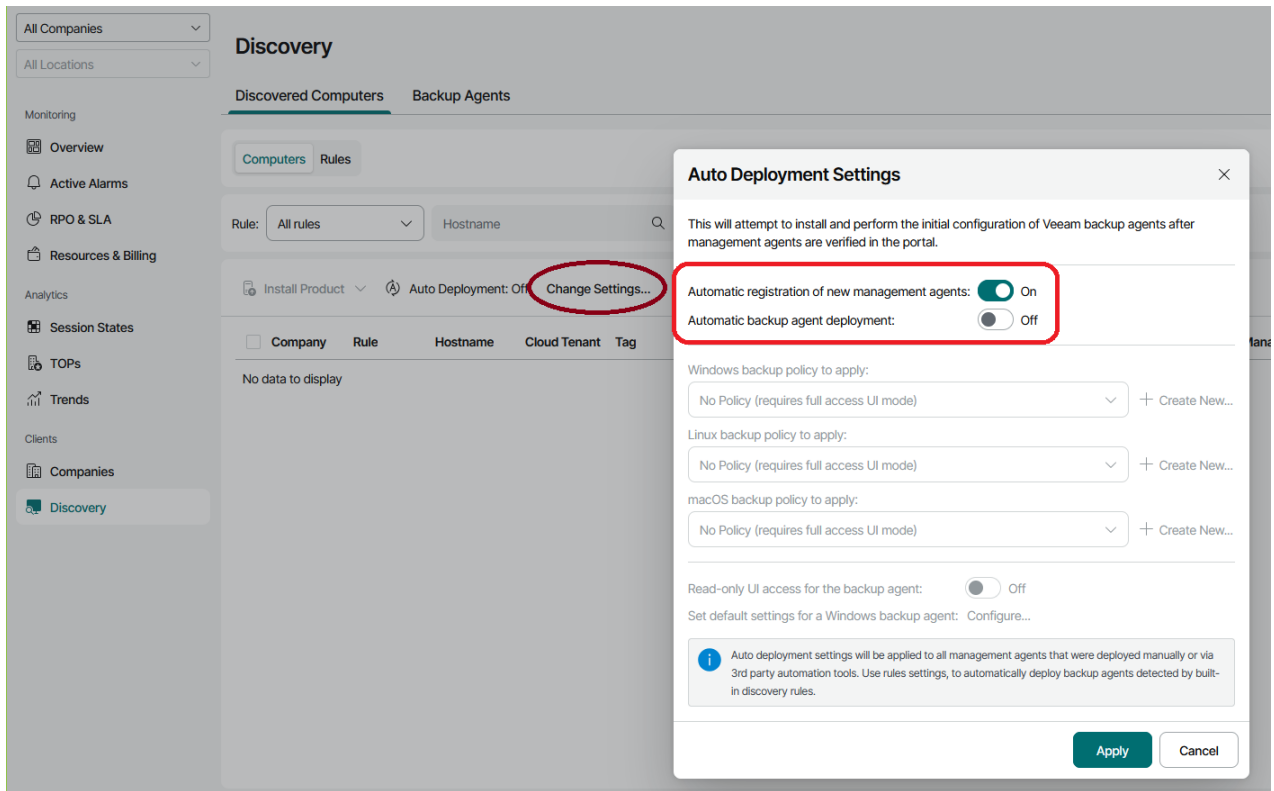
Location: Name

Link: [Create Download Link](#)

Download Cancel

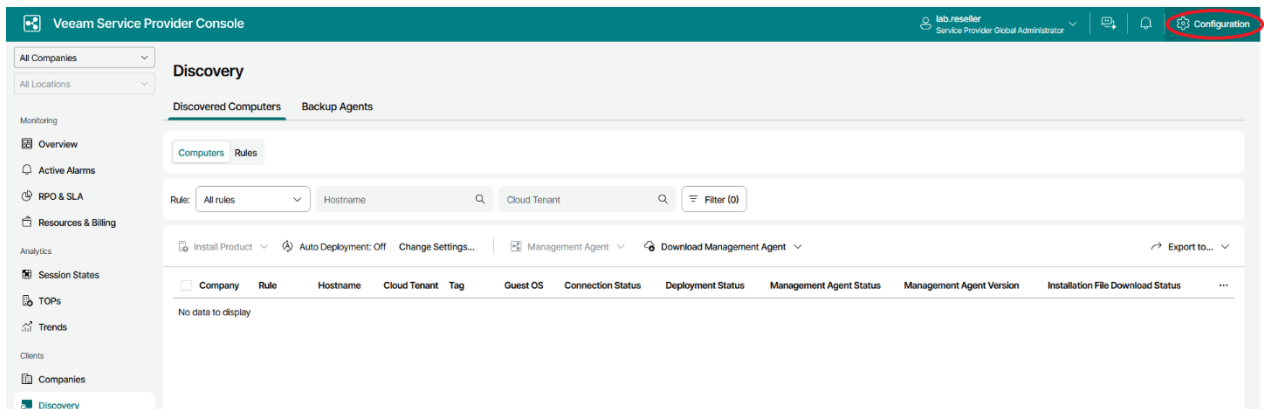
A opção "*Change Settings...*" permite ativar e configurar algumas opções da consola.

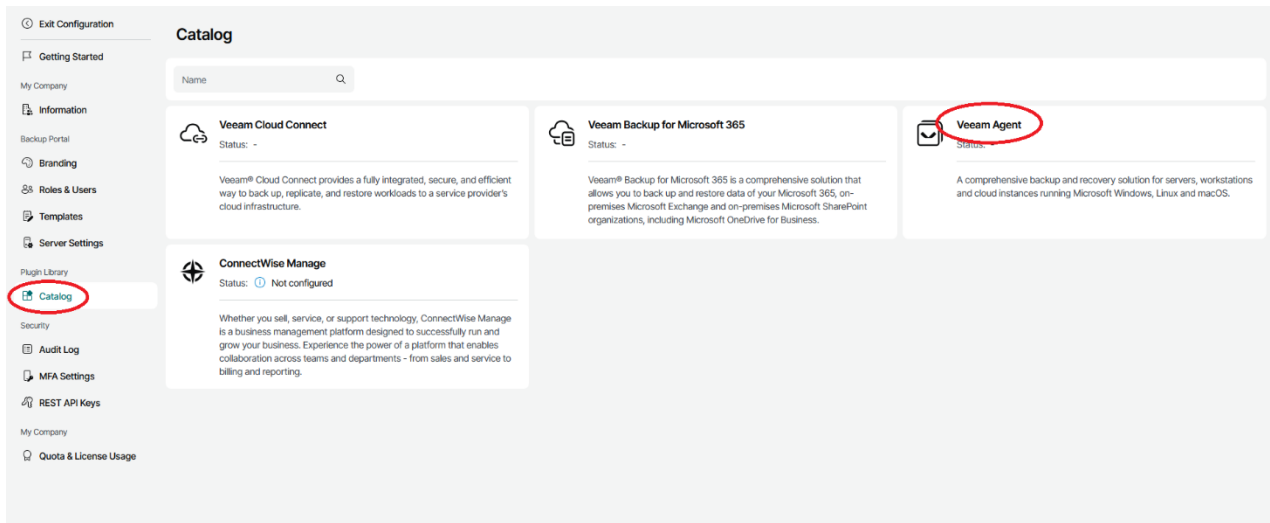
- A opção "*Automatic registration of new management agents*" permite que os agentes de gestão instalados se registem na consola.
- A opção "*Automatic backup agent deployment*" faz com que o agente de backup da Veeam seja instalado automaticamente, e lhe sejam aplicadas determinadas políticas de backup.



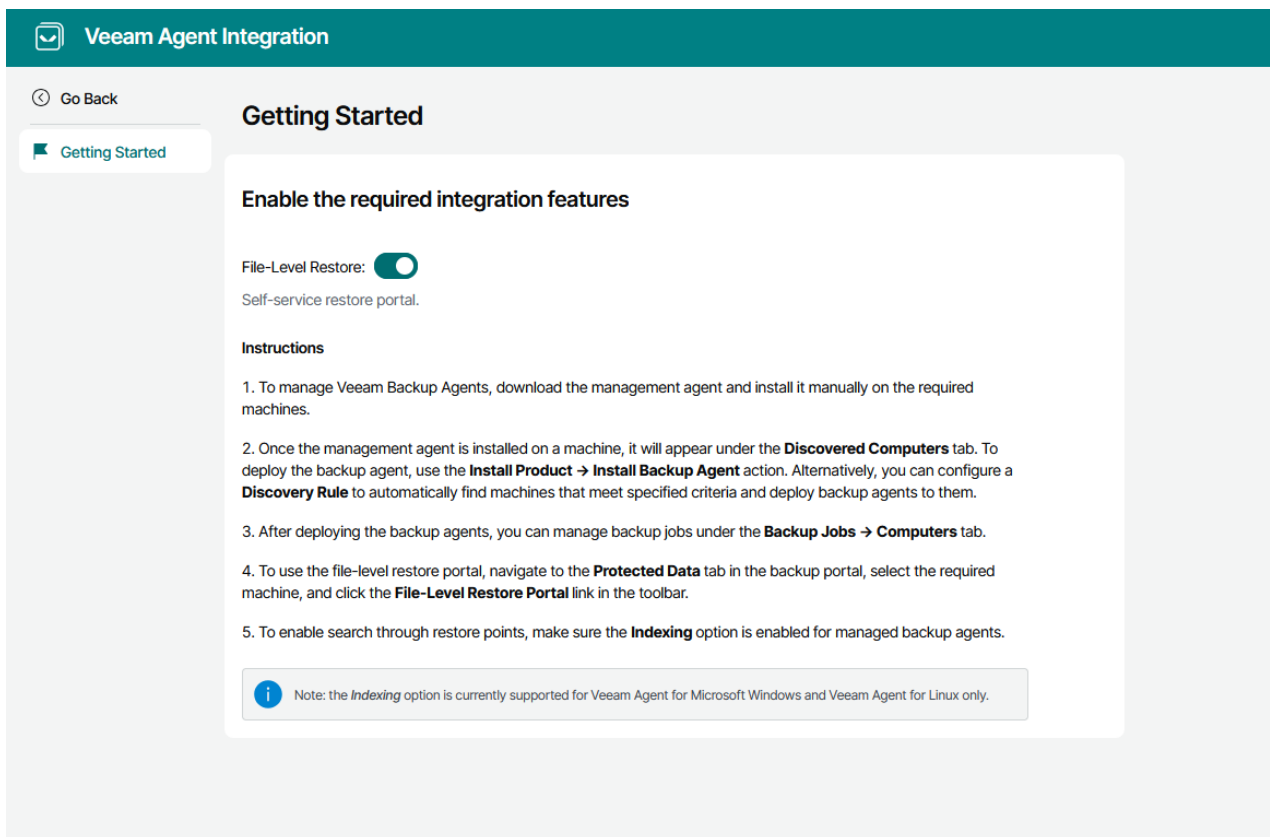
4.7 Ativar portal de restauro self-service

Para que as companhias tenham acesso ao portal de restauro self-service, é necessário ativá-lo como reseller. Para isso, aceder a "Configuration", seguido de "Catalog" no menu lateral esquerdo e depois na área "Veeam Agent":



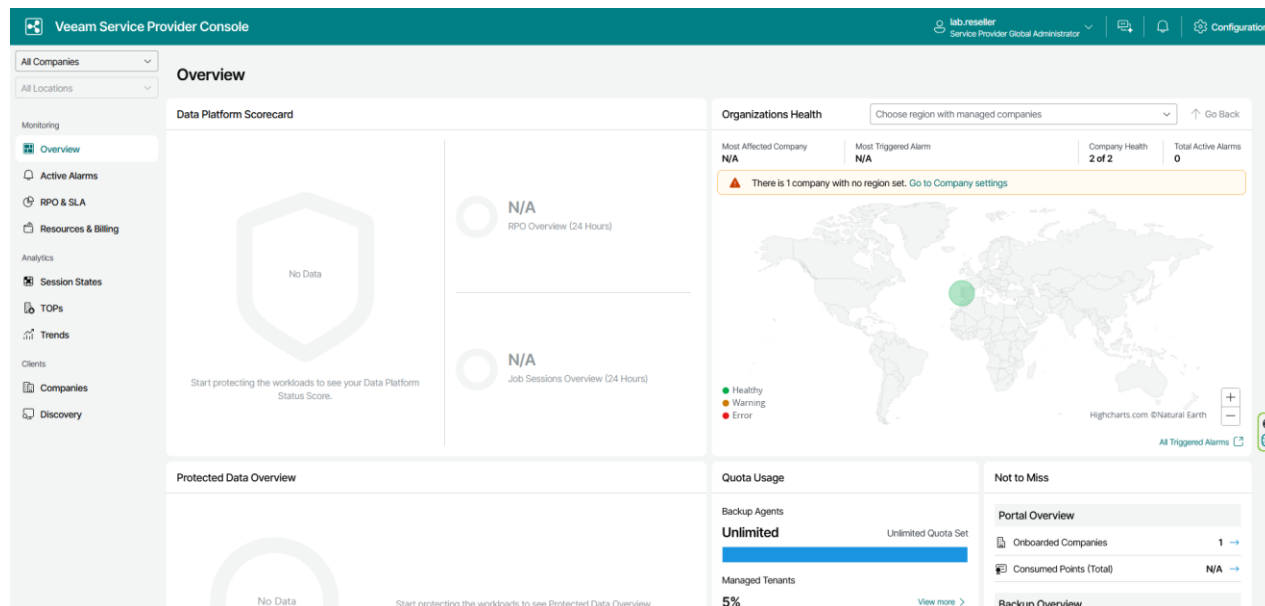


Finalmente, ativar o File-Level Restore:



5. 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.



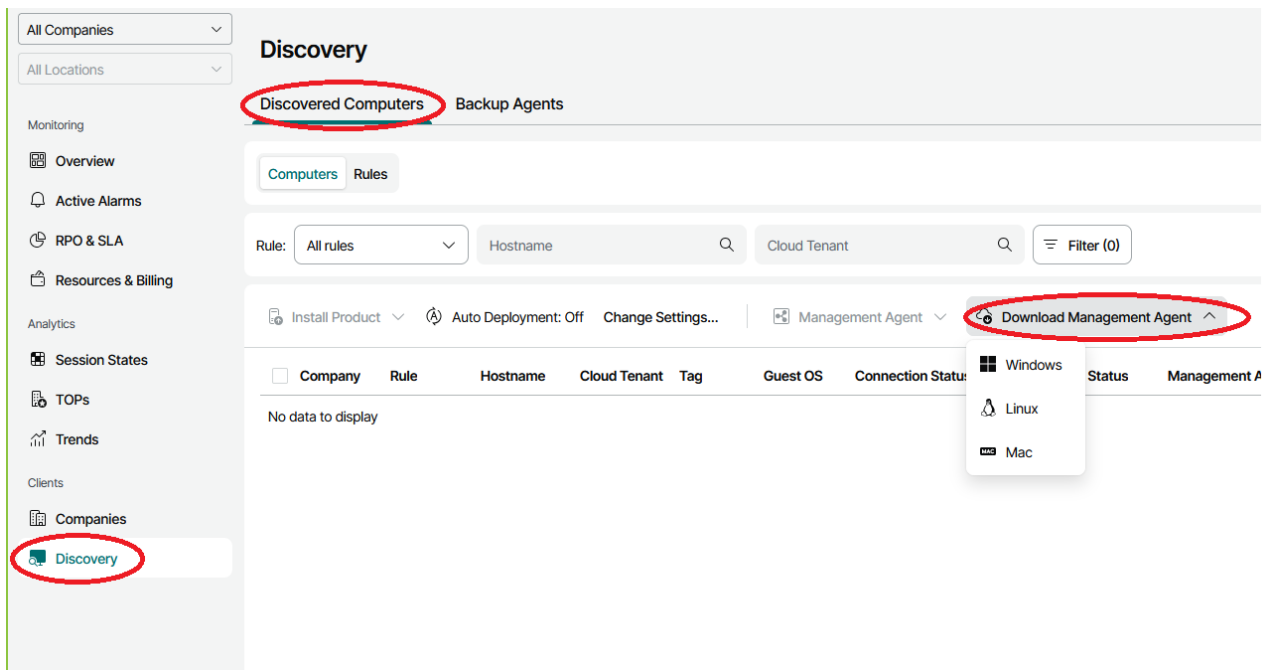
5.1 Instalação do agente de gestão

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

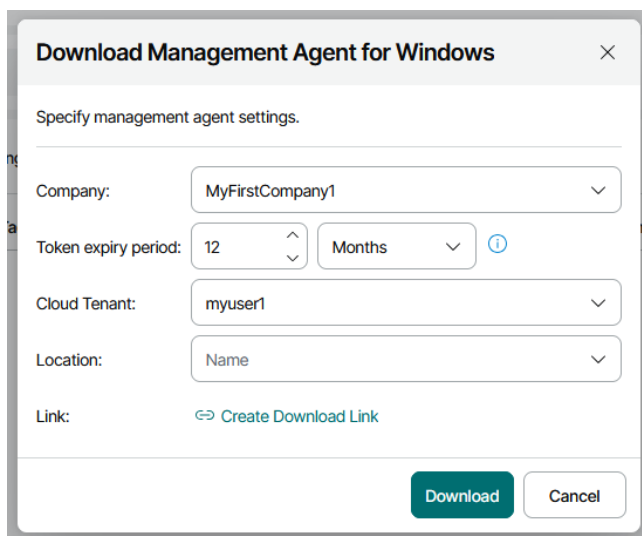
O agente de gestão permite gerir as máquinas físicas ou virtuais que se ligam à plataforma e facilitar o processo de distribuição dos agentes de backup. É responsável pela atualização dos agentes de backup em todas as máquinas que lhe estão inerentes e permite descobrir máquinas físicas ou virtuais em 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, deverá aceder a "Discovery" no menu lateral esquerdo, separador "Discovered Computers" na barra horizontal, seguido de "Download Management Agent", e escolher a plataforma destino pretendida:



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

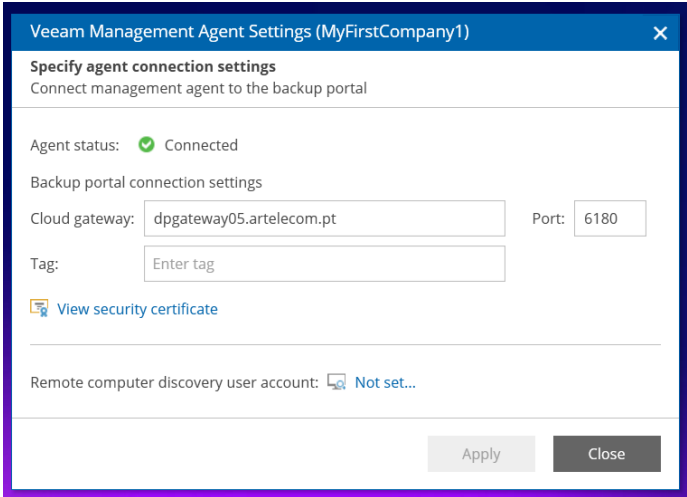
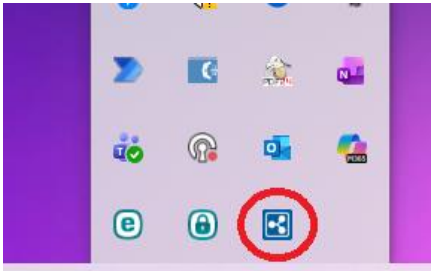


Isto porque o ficheiro a descarregar é específico para a companhia e localização escolhidas. Findo o período de validade do token o instalador deixa de ser válido e é necessário requisitar outro.

5.1.1 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).



5.1.2 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 ~]#
```

5.1.3 Instalar Agente MAC

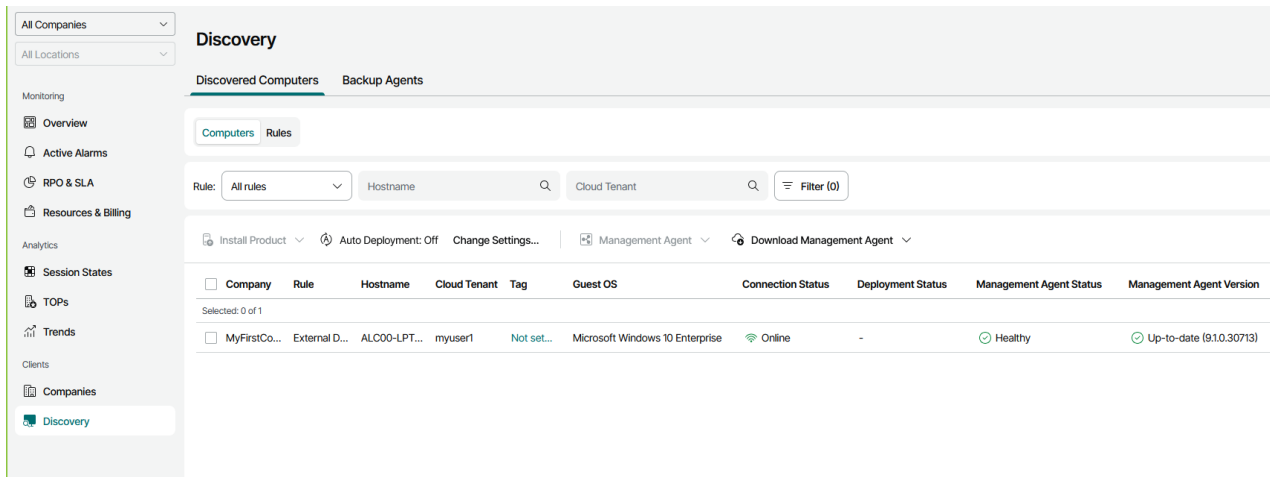
Primeiro executamos o pacote que descarregámos no MAC.

```
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**

5.1.4 Máquinas encontradas e estado dos agentes

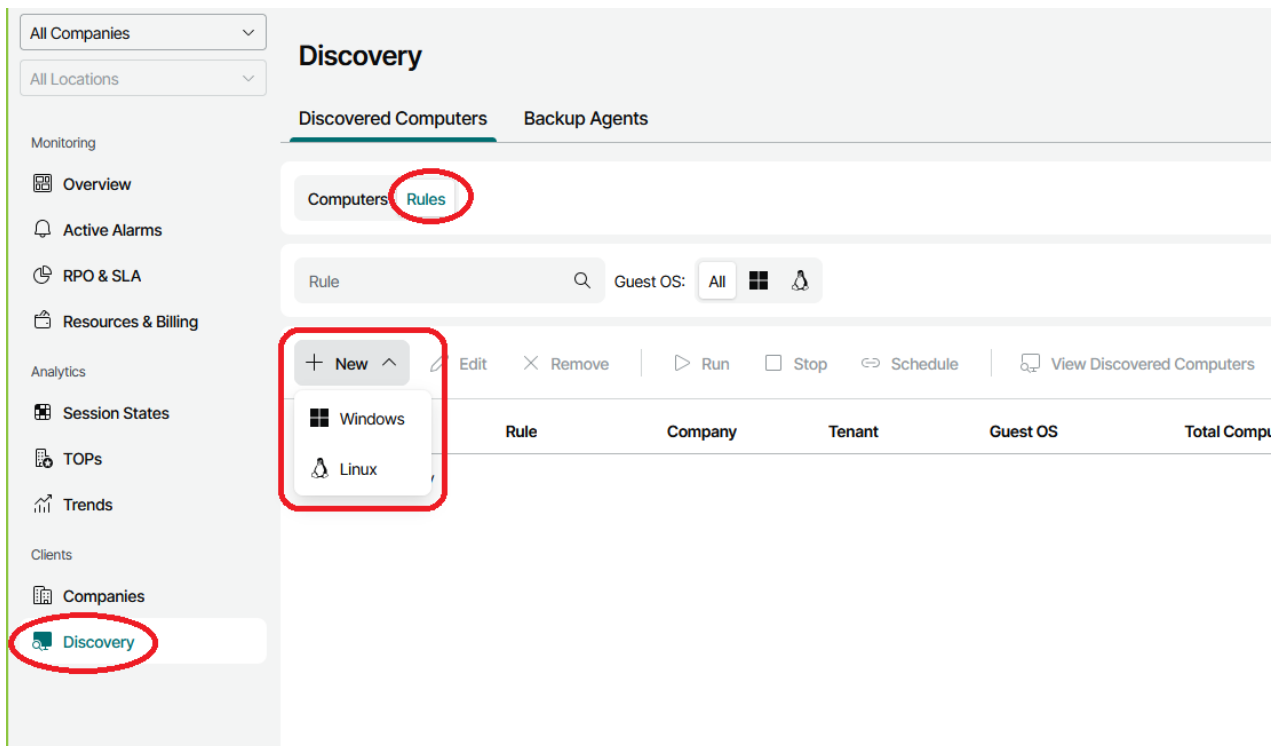
Após a instalação dos agentes de gestão, o quadro "Discovery" apresentará as máquinas com agente instalado, assim como as máquinas descobertas segundo as regras que sejam criadas para o efeito.



5.2 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", no quadro "Discovery", tab "Rules" 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:



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

< Back | **New Windows Discovery Rule**

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

Rule Name
Specify the rule name.

Name:

< Back | **New Windows Discovery Rule**

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

Companies
Select companies to create a discovery rule for.

Company

| <input checked="" type="checkbox"/> Company | Site | Locations |
|---|------------------------------|-----------|
| Selected: 1 of 1 | | |
| <input checked="" type="checkbox"/> MyFirstCompany1 | Ar Telecom - Deep Protection | Remote |

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
- Companies
- 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
- Companies
- Discovery Method
- Network 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
- Companies
- Discovery Method
- Network 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
- Companies
- Discovery Method
- Network 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
- Companies
- Discovery Method
- Network 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

i Backup agent deployment and management has been disabled for the company

Backup policy to apply: Workstation: File level backup, Personal files, Local + Create New... Show

Read-only UI access for the backup agent: On

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

i 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
- Companies
- Discovery Method
- Network 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...

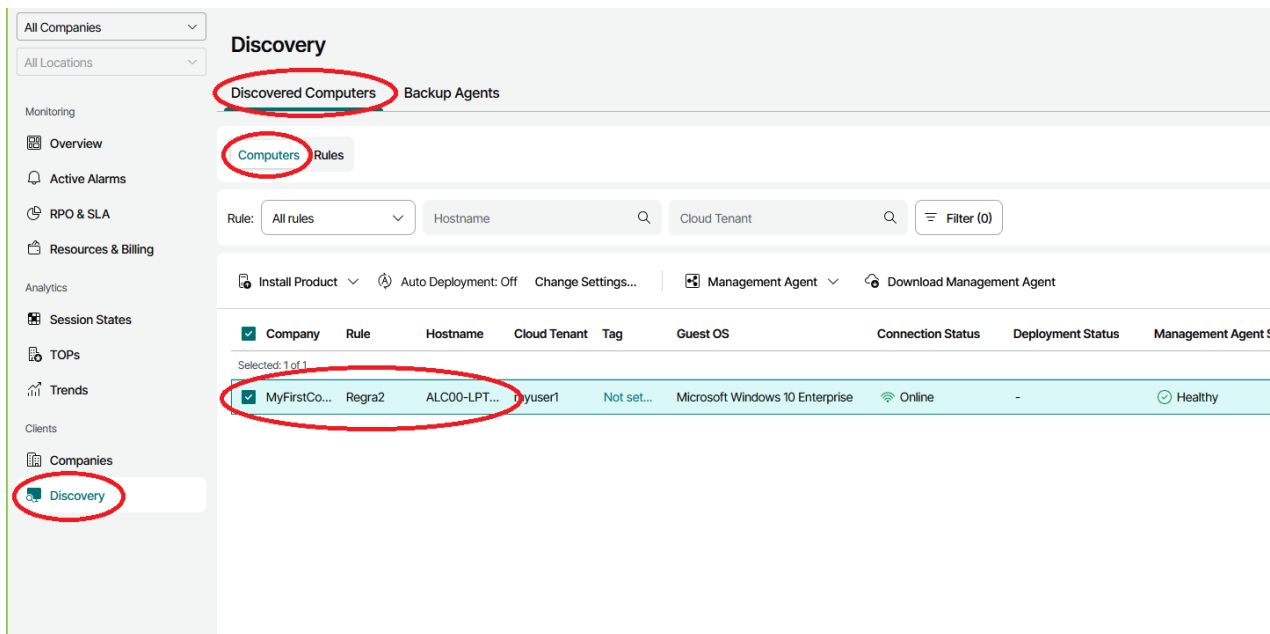
Periodically every: 1 ▼ Hours ▼

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

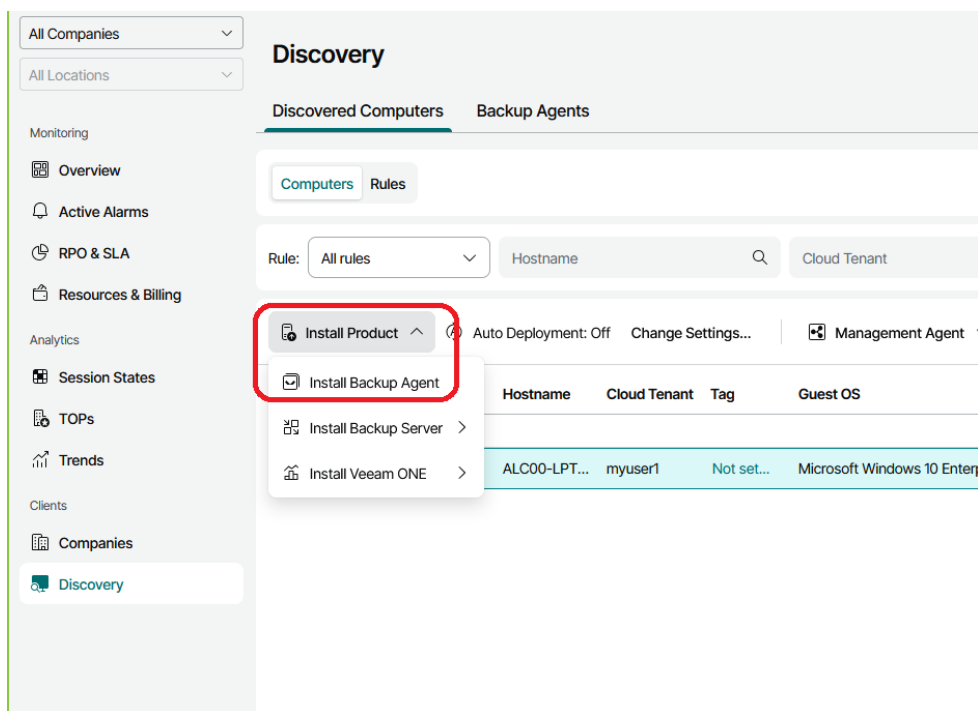
Terminadas as configurações, validam-se os dados introduzidos gravando a regra e permitindo a sua execução imediata.

5.3 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, no quadro "Discovery", tab "Discovered Computers" e "Computers", seleccionar primeiro o servidor ou workstation onde se quer instalar o agente de backup:



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.



Install Backup Agent - ALC00-LPT262

This operation will attempt to install and perform initial configuration of Veeam backup agents.
To start this operation, specify local administration credentials to use.

Use guest OS credentials from:

Account specified in the discovery rule or in the management agent settings

The following user account: + New

Backup policy to apply:

+ Create New...

Read-only UI access for the backup agent: On

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

i 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.



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

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

The screenshot shows the 'Discovery' section of the Ar Cloud interface. It features a sidebar with navigation options like 'Monitoring', 'Analytics', and 'Clients'. The main area is titled 'Discovery' and has tabs for 'Discovered Computers' and 'Backup Agents'. Under 'Discovered Computers', there are search filters for 'Rule', 'Hostname', and 'Cloud Tenant'. Below the filters, there are controls for 'Install Product', 'Auto Deployment: Off', and 'Management Agent'. A table lists discovered computers with columns for Company, Rule, Hostname, Cloud Tenant, Tag, Guest OS, Connection Status, Deployment Status, and Management Agent Status. One computer, 'myuser1', is shown with a deployment status of 'Installing...'.

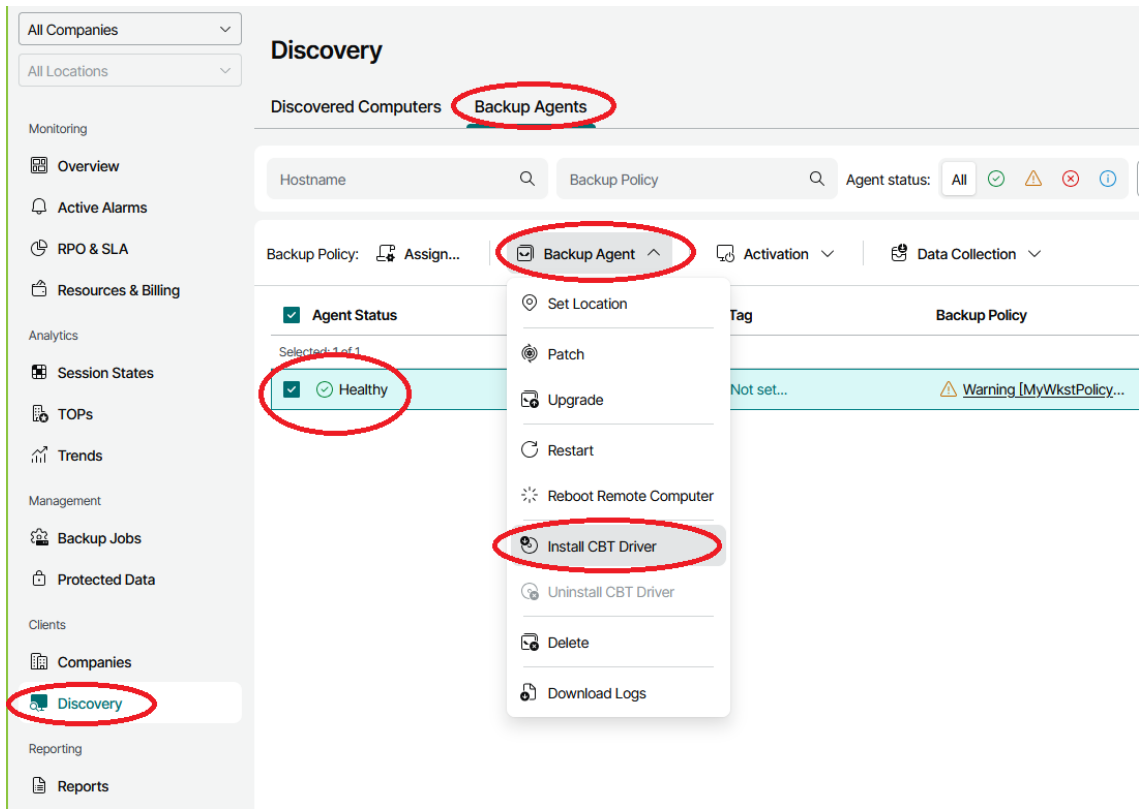
| Company | Rule | Hostname | Cloud Tenant | Tag | Guest OS | Connection Status | Deployment Status | Management Agent Status |
|--------------|--------|--------------|--------------|------------|---------------------------------|-------------------|-------------------|-------------------------|
| MyFirstCo... | Regra2 | ALC00-LPT... | myuser1 | Not set... | Microsoft Windows 10 Enterprise | Online | Installing... | Healthy |

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

The screenshot shows a 'Task Details' dialog box for task 'ALC00-LPT262'. It includes a progress bar at 5% and buttons for 'Download Logs', 'Copy All to Clipboard', and 'Cancel Deployment'. Below the progress bar is a table of actions:

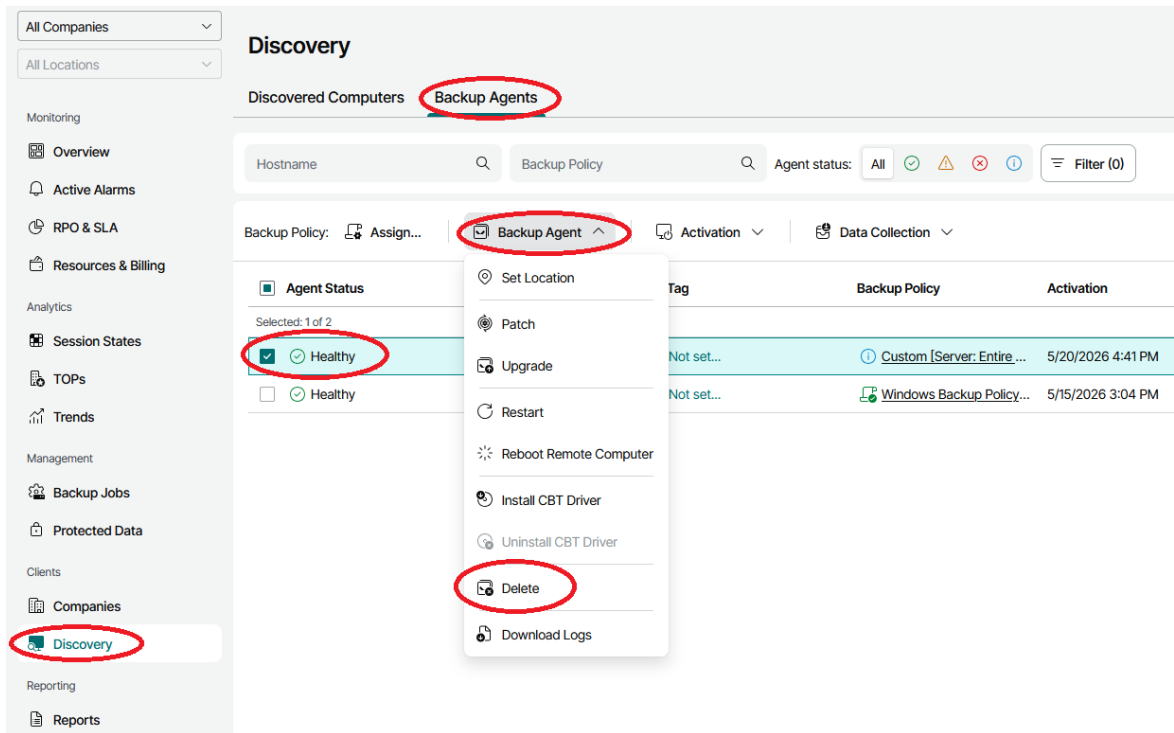
| Action | Start Time | End Time | Duration |
|--|-------------------|-------------------|------------|
| Adding task to the queue | 5/15/2026 3:01 PM | 5/15/2026 3:01 PM | 4 Seconds |
| Uploading backup agent to the computer | 5/15/2026 3:01 PM | 5/15/2026 3:01 PM | 3 Seconds |
| Downloading files 1 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 | - | - |

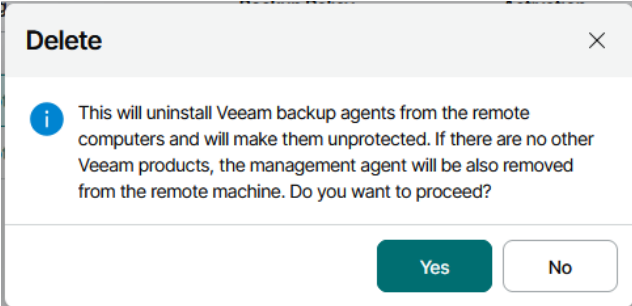
É possível ativar a funcionalidade "CBT Driver" da Veeam (Changed Block Tracking) que facilita o backup incremental. Este driver pode ser instalado com a máquina a funcionar, mas apenas ficará ativo após um reinício da mesma. No quadro "Discovery", tab "Backup Agents", selecionar primeiro o servidor ou workstation onde se quer instalar o agente de backup e de seguida instalar o driver CBT:



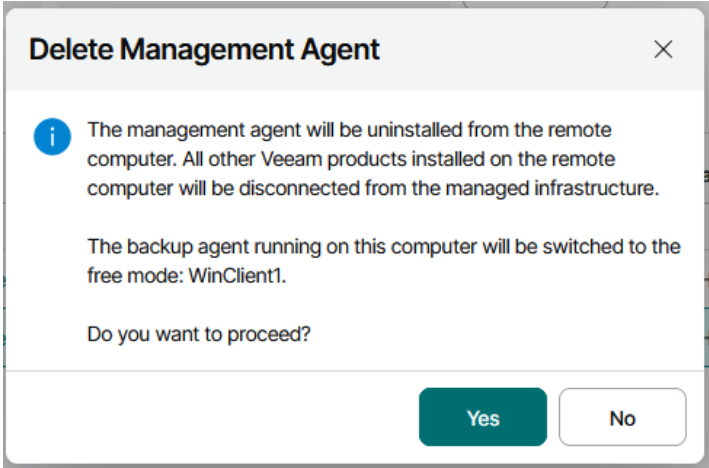
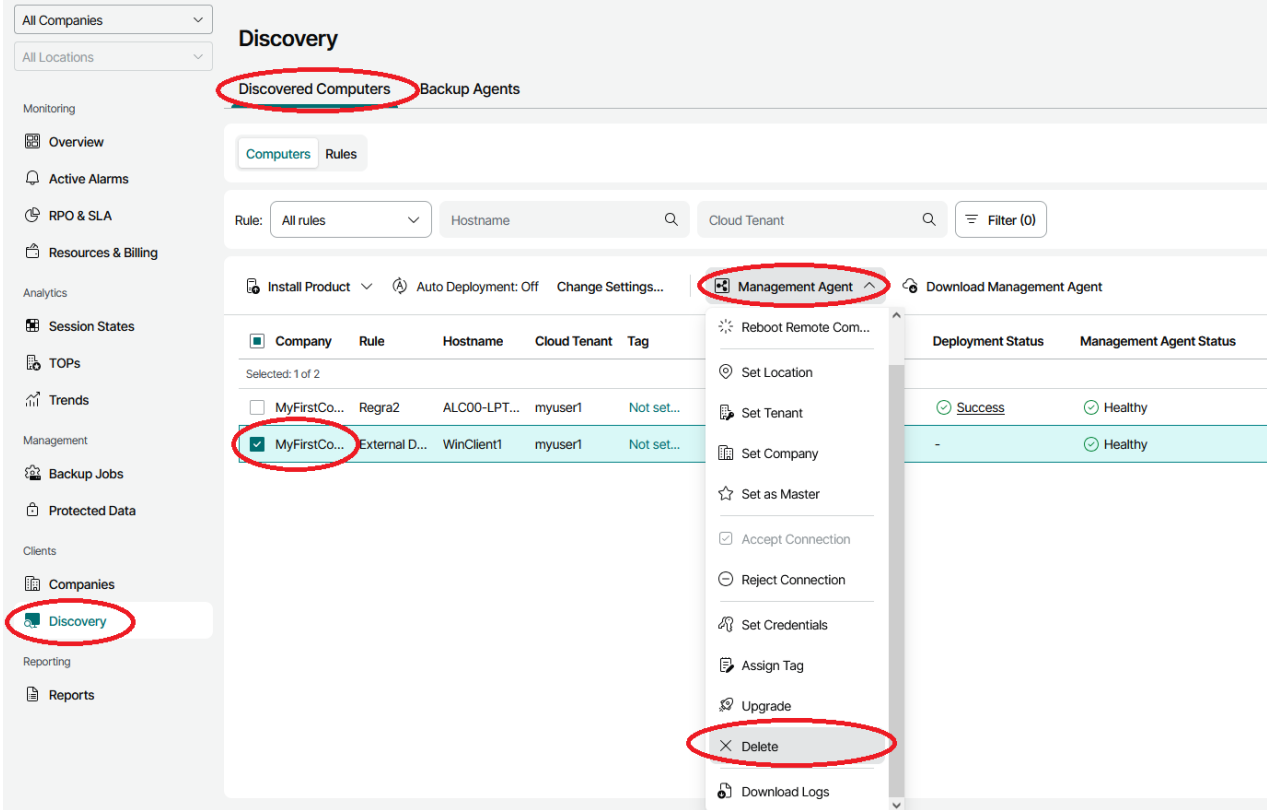
5.4 Remoção de agentes

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

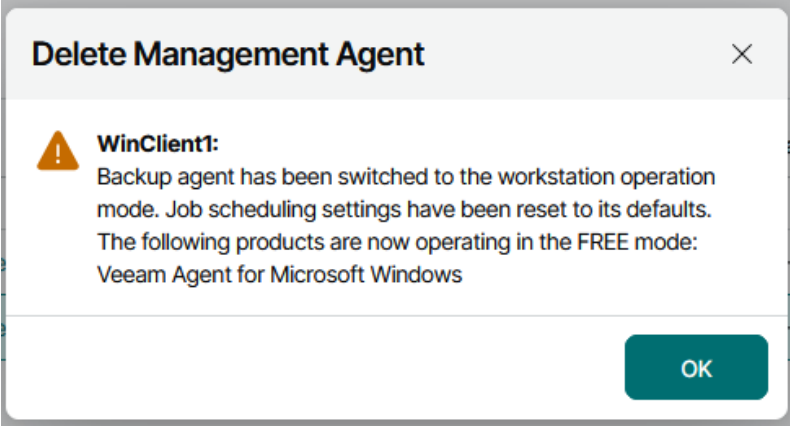




Ao remover o agente de backup também é removido o agente de gestão.
Para remover apenas o agente de gestão:

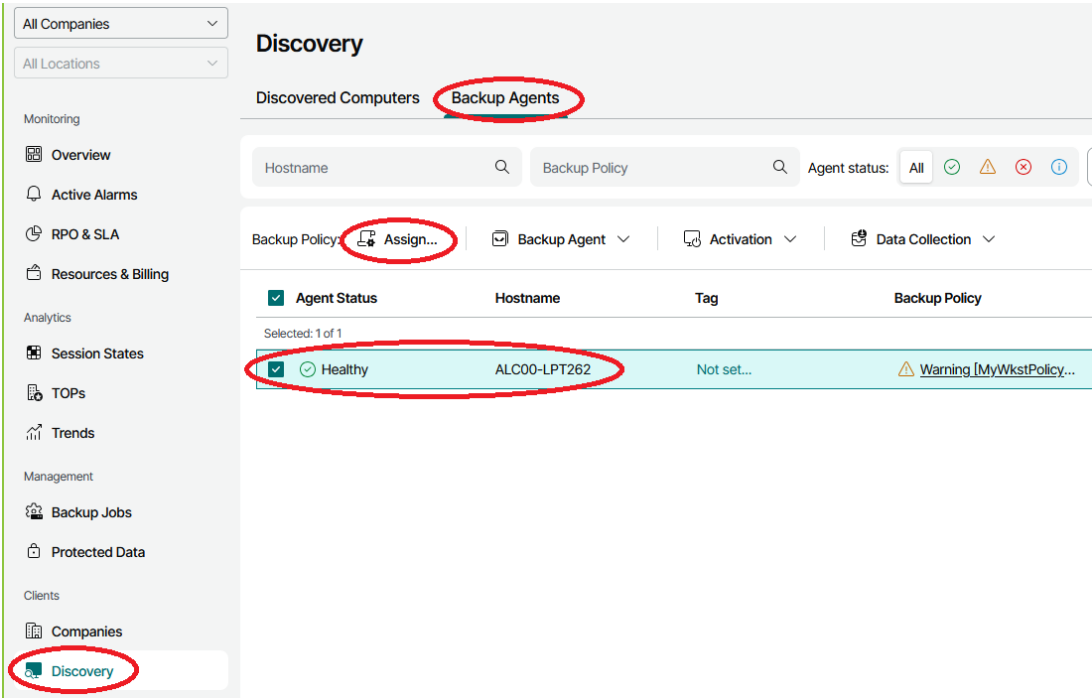


Se o agente de gestão for desinstalado sem desinstalar primeiro o agente de backup, então os agentes de backup geridos por ele ficarão a funcionar em modo "Free", o que quer dizer que deixam de ter acesso ao repositório remoto da Ar. Podem ser usados para efetuar backups e restauros locais. A partir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



5.5 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, no quadro "Discovery", tab "Backup Agents", selecionar primeiro o servidor ou workstation e assignar uma política, caso não tenha sido selecionado na fase de instalação do agente de backup.



| <input checked="" type="checkbox"/> | Name | Type | Policy Type | Created by | Description |
|-------------------------------------|------------------------------|-------------|---------------------|--------------|-----------------------------|
| <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 | - |

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: | | |

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

Assigned Backup Policies - ALC00-LPT262

Backup Policy Type: All

| <input checked="" type="checkbox"/> Name | Type | Description |
|---|------|-------------|
| <input checked="" type="checkbox"/> ⚠ Warning [Workstation: File | | |

Selected: 1 of 1

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.

5.6 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:

| Name | Type | Policy Type | Created by | Description |
|------------------------------|-------------|---------------------|--------------|-----------------------------|
| Workstation: File level b... | Workstation | Created by Provider | Ar Telecom | This policy processes u... |
| Server: Entire computer... | Server | Created by Provider | Ar Telecom | This policy should be us... |
| MyWkstPolicy2 | Workstation | Created by Reseller | LAB_RESELLER | - |

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

| Policy | Access Type | Policy Type | Guest OS | Operation Mode | Companies | Modified Date | Created by | Description |
|--|-------------|---------------------|----------|----------------|-----------|---------------------|--------------|----------------------------|
| Linux server - Entire computer | Public | Created by Provider | Linux | Server | 0 | 4/17/2026 5:31 PM | Ar Telecom | This policy should be u... |
| Linux workstation - Home directory | Public | Created by Provider | Linux | Workstation | 0 | 10/13/2021 10:50 AM | Ar Telecom | This policy processes /... |
| Mac server - Entire computer | Public | Created by Provider | macOS | Server | 0 | 10/13/2021 10:50 AM | Ar Telecom | This policy should be u... |
| Mac workstation - Users directory | Public | Created by Provider | macOS | Workstation | 0 | 10/13/2021 10:50 AM | Ar Telecom | This policy processes /... |
| MyWkstPolicy2 | Private | Created by Reseller | Windows | Workstation | 0 | 9/10/2024 11:11 AM | LAB_RESELLER | - |
| Server: Entire computer. Microsoft E... | Public | Created by Provider | Windows | Server | 0 | 5/8/2019 3:27 PM | Ar Telecom | This policy should be u... |
| Windows Backup Policy 4 | Public | Created by Reseller | Windows | Server | 1 | 5/15/2026 4:04 PM | LAB_RESELLER | Created by Service Pro... |
| Workstation: File level backup. Perso... | Public | Created by Provider | Windows | Workstation | 0 | 5/8/2019 3:27 PM | Ar Telecom | This policy processes u... |



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":

Templates

Subscription Plans | **Backup Policies** | Predefined Alarms

Policy Filter (None)

+ New Edit Copy Remove Propagate Changes

| Policy ↑ | Access Type | Policy Type | Guest OS | Operation Mo |
|--|-------------|---------------------|----------|--------------|
| Linux server - Entire computer | Public | Created by Provider | Linux | Server |
| Linux workstation - Home directory | Public | Created by Provider | Linux | Workstation |
| Mac server - Entire computer | Public | Created by Provider | macOS | Server |
| Mac workstation - Users directory | Public | Created by Provider | macOS | Workstation |
| MyWkstPolicy2 | Private | Created by Reseller | Windows | Workstation |
| Server: Entire computer. Microsoft Exchange Server. Cloud bac... | Public | Created by Provider | Windows | Server |
| Windows Backup Policy 4 | Public | Created by Reseller | Windows | Server |
| Workstation: File level backup. Personal files. Local drive. Daily ... | Public | Created by Provider | Windows | Workstation |
| Workstation: File level backup. Personal files. Local drive. Daily ... | Public | Created by Reseller | Windows | Workstation |

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

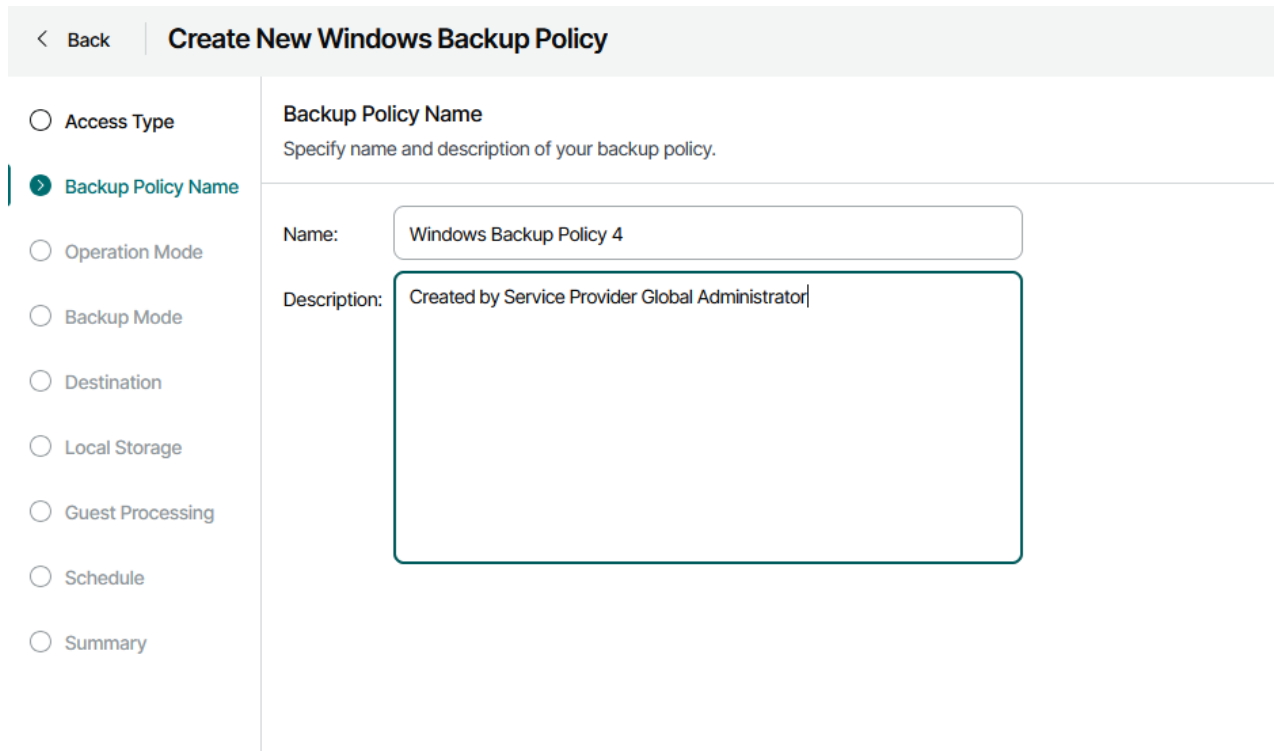
- Access Type**

Select backup policy access type.

 - Public**
This policy will be visible to every managed company.
 - Private**
This policy will be visible only to companies which this policy is assigned to.
- Backup Policy Name
- Operation Mode
- Backup Mode
- Destination
- Local Storage
- Guest Processing
- Schedule
- Summary

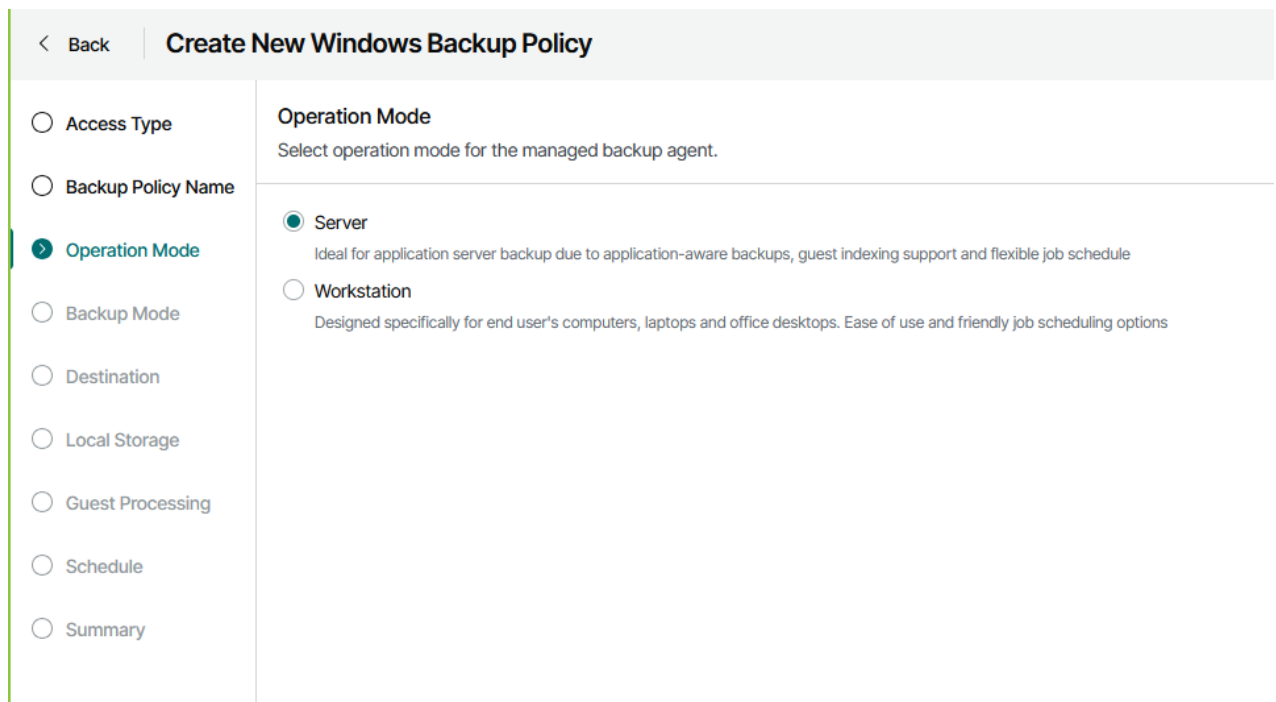
Ao criar uma política é dado a escolher qual o sistema operativo a que se destina: Windows, Linux ou Mac.

O primeiro passo é dar um nome à política a criar:



The screenshot shows the 'Create New Windows Backup Policy' interface. On the left is a vertical navigation menu with radio buttons for: Access Type, Backup Policy Name (selected), Operation Mode, Backup Mode, Destination, Local Storage, Guest Processing, Schedule, and Summary. The main content area is titled 'Backup Policy Name' and includes the instruction 'Specify name and description of your backup policy.' Below this, there are two input fields: 'Name:' with the value 'Windows Backup Policy 4' and 'Description:' with the value 'Created by Service Provider Global Administrator|'.

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.



The screenshot shows the 'Create New Windows Backup Policy' interface at the 'Operation Mode' step. The left navigation menu now has 'Operation Mode' selected. The main content area is titled 'Operation Mode' and includes the instruction 'Select operation mode for the managed backup agent.' There are two radio button options: 'Server' (selected) with the description 'Ideal for application server backup due to application-aware backups, guest indexing support and flexible job schedule', and 'Workstation' with the description '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, aplicativo ou granular;
- **Volume level backup:** faz backup apenas dos volumes selecionados;
- **File level backup:** backup de pastas e ficheiros.

< Back
Create New Windows Backup Policy

- Access Type
- 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**

- Access Type
- 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 back up in the following format "C:\":

C:\

Back up all volumes except

Type in the name of the volume you want to exclude from backup in the following format "C:\":

C:\

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**

Access Type

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**

- Access Type
- Backup Policy Name
- Operation Mode
- Backup Mode
- Files
- 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**

- Access Type
- Backup Policy Name
- Operation Mode
- Backup Mode
- Files
- 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: January, February,...

Weekly on selected days:

Active full backup

Create active full backups periodically **i**

Monthly on: January, February,...

Weekly on selected days:

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**

- Access Type
- Backup Policy Name
- Operation Mode
- Backup Mode
- Files
- 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: 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.

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

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

Guest Processing
Choose Guest OS processing 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.

Customize 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...

Processing Settings

General **SQL** Oracle SharePoint Scripts

Specify Microsoft SQL Server account with database admin privileges:

Username:

Password:

Choose how this job should process Microsoft SQL Server transaction logs.

Truncate logs (prevents logs from growing forever)

Do not truncate logs (requires simple recovery model)

Backup logs periodically (backed up logs are truncated)

Backup logs every: minutes

Retain log backups:

Until the corresponding image-level backup is deleted

Keep only last: days of log backups

No último passo configura-se o agendamento dos backups.

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

- Access Type
- Backup Policy Name
- Operation Mode
- Backup Mode
- Files
- 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:

Monthly at this time:

Periodically every:

Automatic retry

Retry failed job: times

Wait before each retry for: minutes

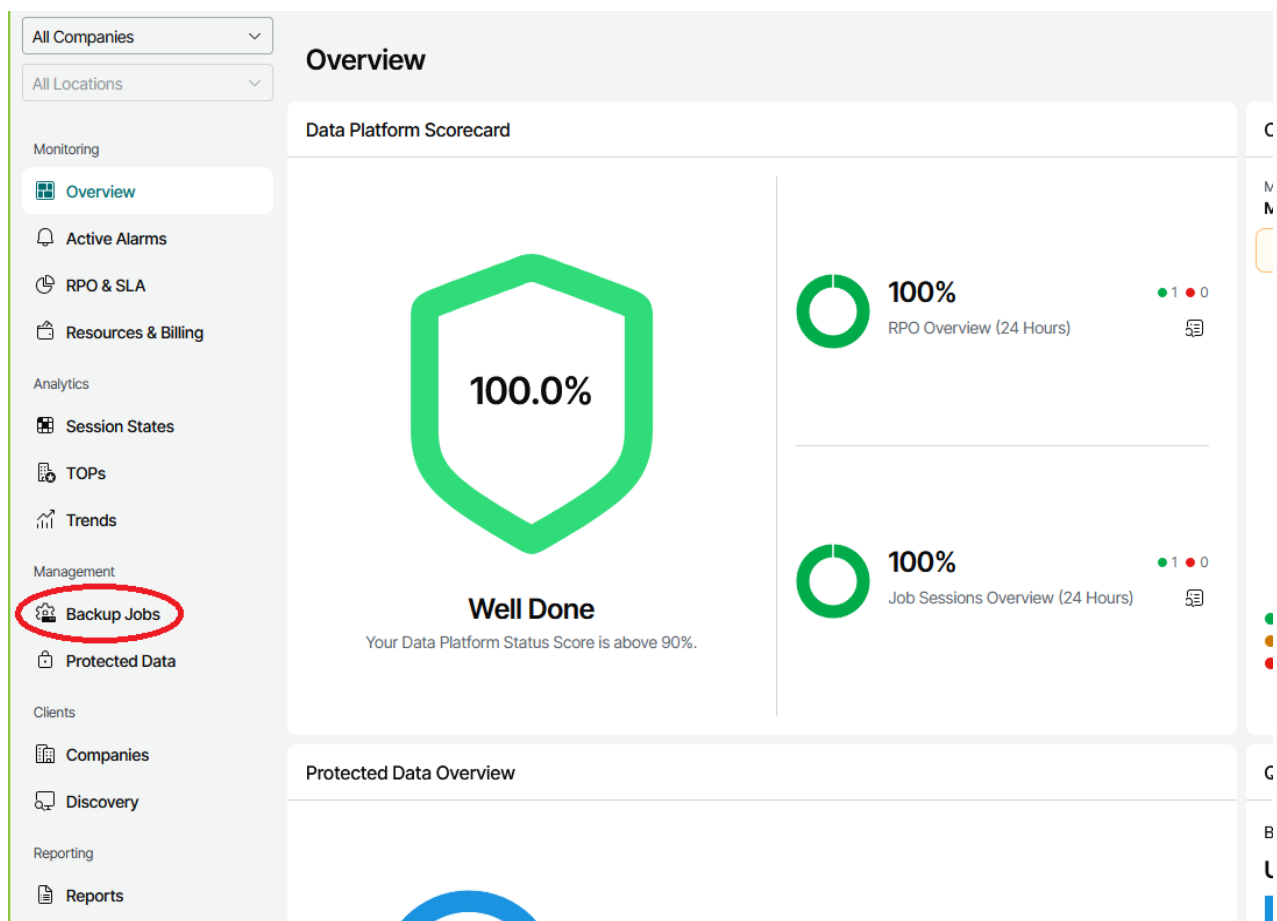
Terminate job if it exceeds allowed backup window

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.

5.7 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.

Backup Jobs

Computer | Status: All 🟢 🟡 🔴 🟢 🟡 🟢 | Filter (0)

Actions | + Create Job | Backup Agent UI | Scheduling | Settings | Download Logs

| Company | Tenant | Computer | Tag | Operation Mode | Successful Jobs | Running Jobs | Backup Policy |
|--|---------|--------------|------------|----------------|-----------------|--------------|---------------------|
| Selected: 0 of 1 | | | | | | | |
| <input type="checkbox"/> MyFirstCompany1 | myuser1 | ALC00-LPT262 | Not set... | Server | 🟢 1 of 1 | 🔴 0 of 1 | 🟢 Windows Backup... |

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:

Agent Backup Job - ALC00-LPT262

Job name | Status: All 🟢 🟡 🔴 🟢 🟡 🟢 | 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 |
|------------------------------------|--------------------------------|---------------|-----------------------------|----------------|-------------|------------|----------------|---------------|
| Selected: 0 of 1 | | | | | | | | |
| <input type="checkbox"/> 🟢 Success | Windows Backup Policy 4_ALC... | 🟢 Window... | myuser1_ALC00-LPT262_Rep... | 8 | 29.5 GB | Daily | 22 minutes ... | Offsite |

OK

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 |
|---------------|--------------------------------|---------------|-----------------------------|----------------|-------------|------------|----------------|---------------|
| 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

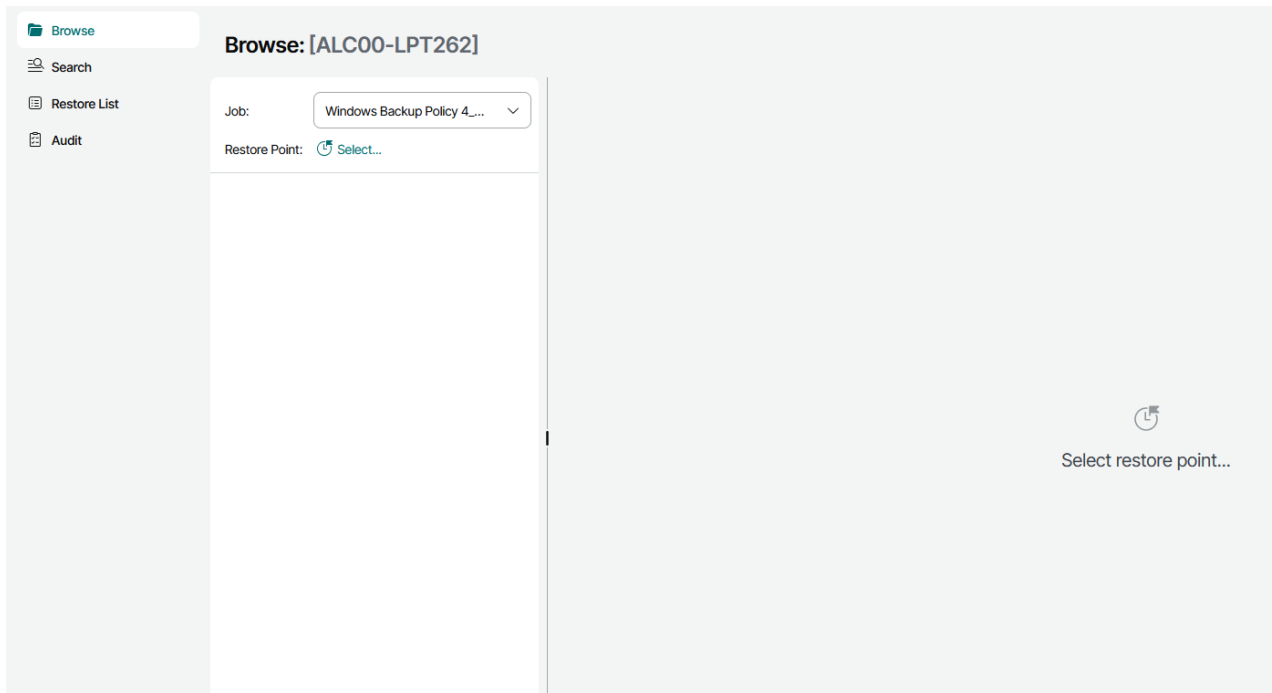
5.8 Recuperação granular de ficheiros via portal

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

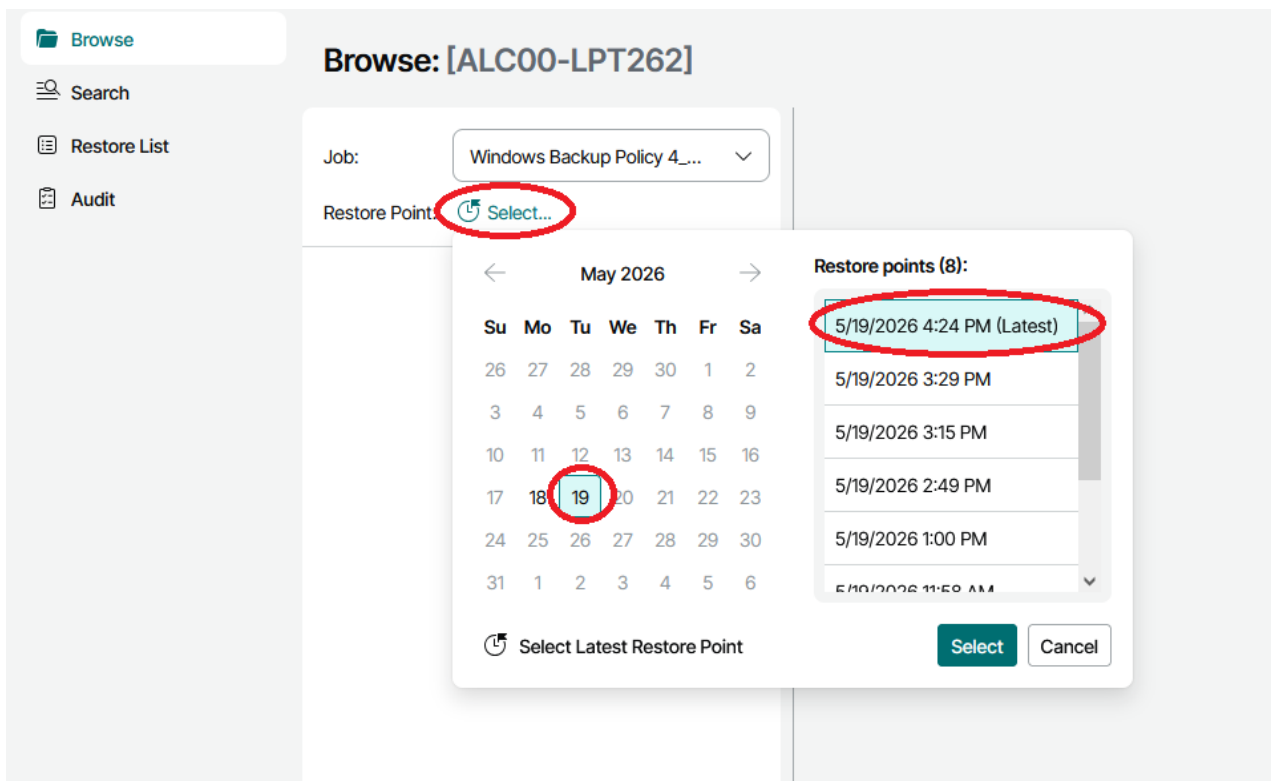
Para efetuar um restauro, deve-se selecionar a máquina pretendida e em seguida "File-Level Restore Portal":

| <input checked="" type="checkbox"/> | Name ↑ | Backup Stat... | Tag | Backups | Backup Copies | Guest OS | Latest Restore Point | Cloud Copy |
|-------------------------------------|--------------|----------------|------------|---------|---------------|-----------------|----------------------|------------------|
| <input checked="" type="checkbox"/> | ALC00-LPT262 | Active | Not set... | 1 | - | Microsoft Wi... | 40 minutes ago | Yes (40 minute.. |

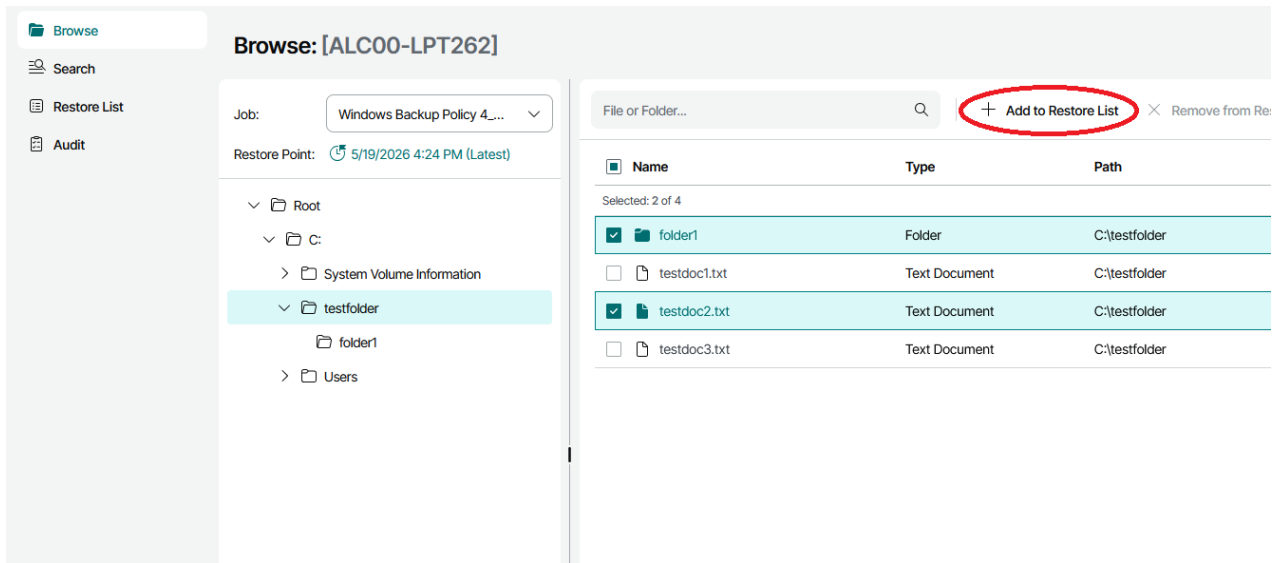
Isto leva-nos ao portal de restauro:



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]

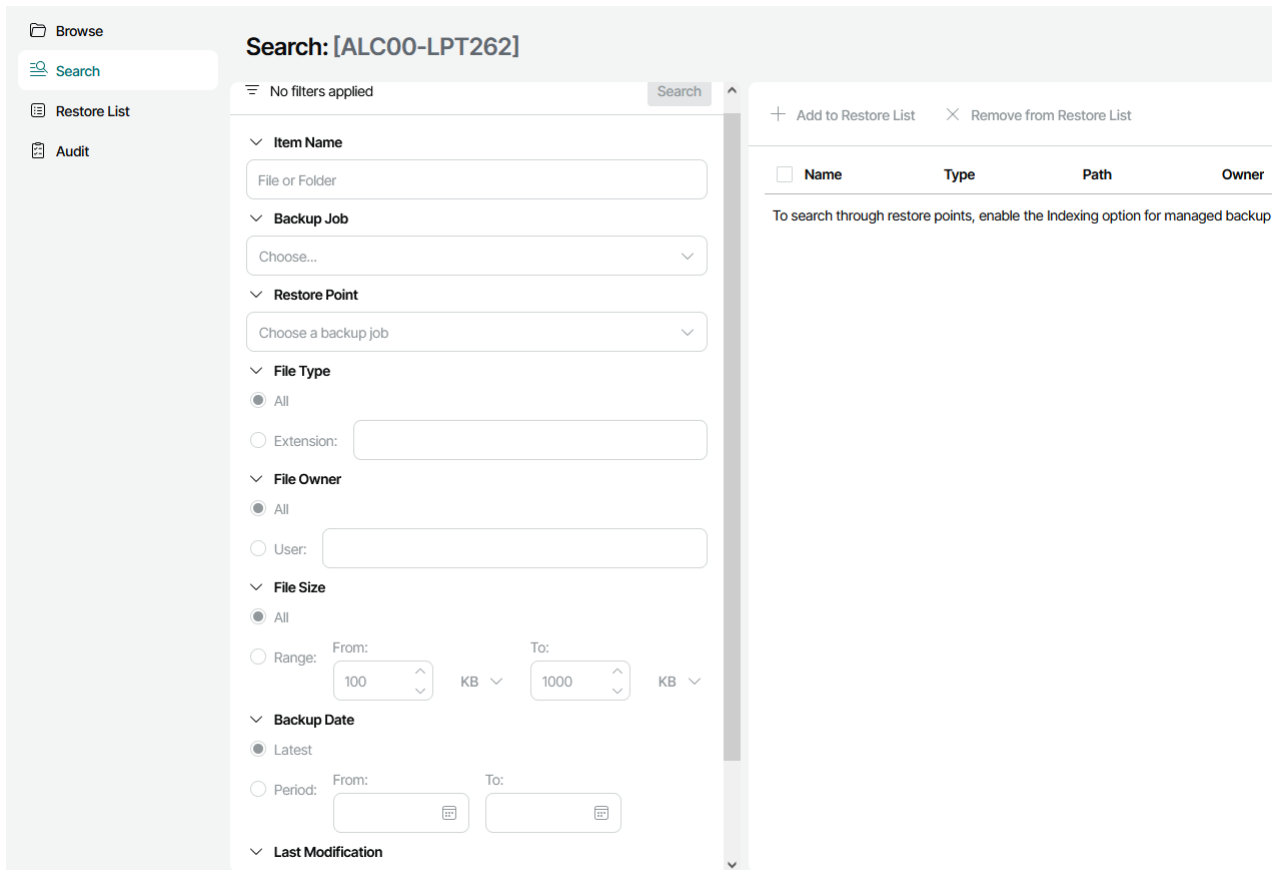
Job: Windows Backup Policy 4...

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]

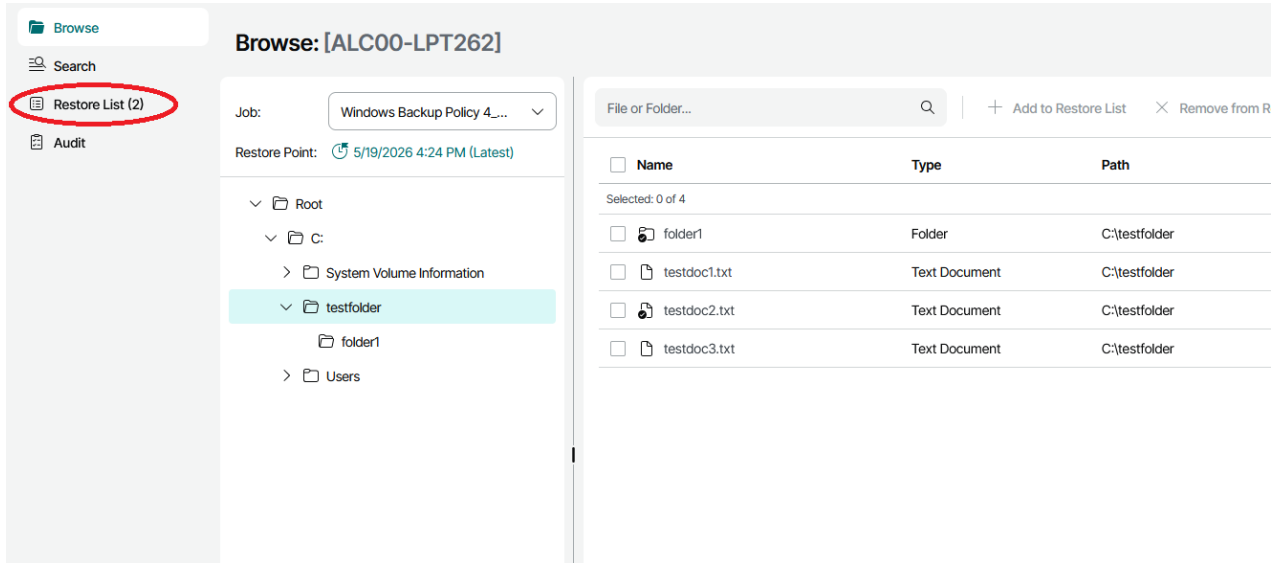
No filters applied

| 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:



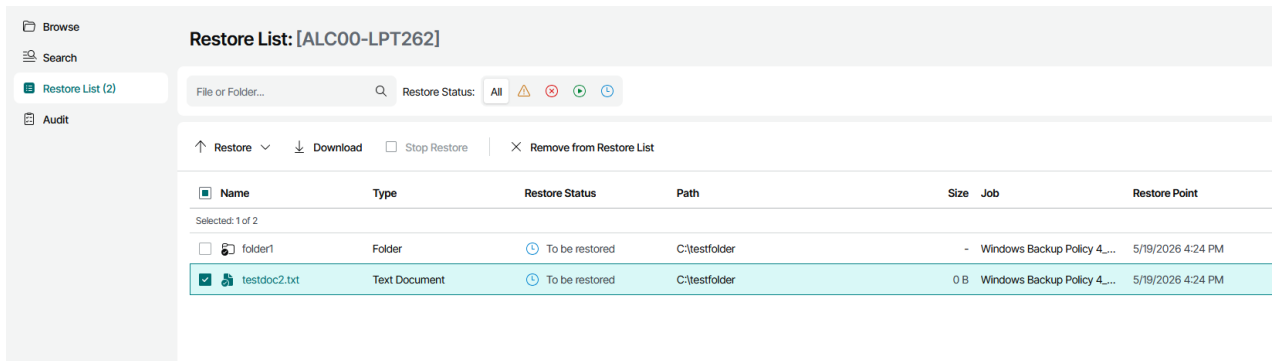
Browse: [ALC00-LPT262]

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

File or Folder... | + Add to Restore List | × 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.



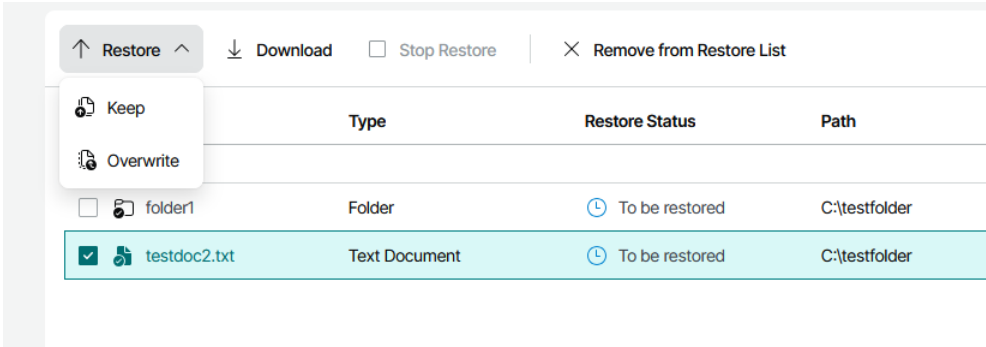
Restore List: [ALC00-LPT262]

File or Folder... | Restore Status: All | ⚠ | ⛔ | ⌛

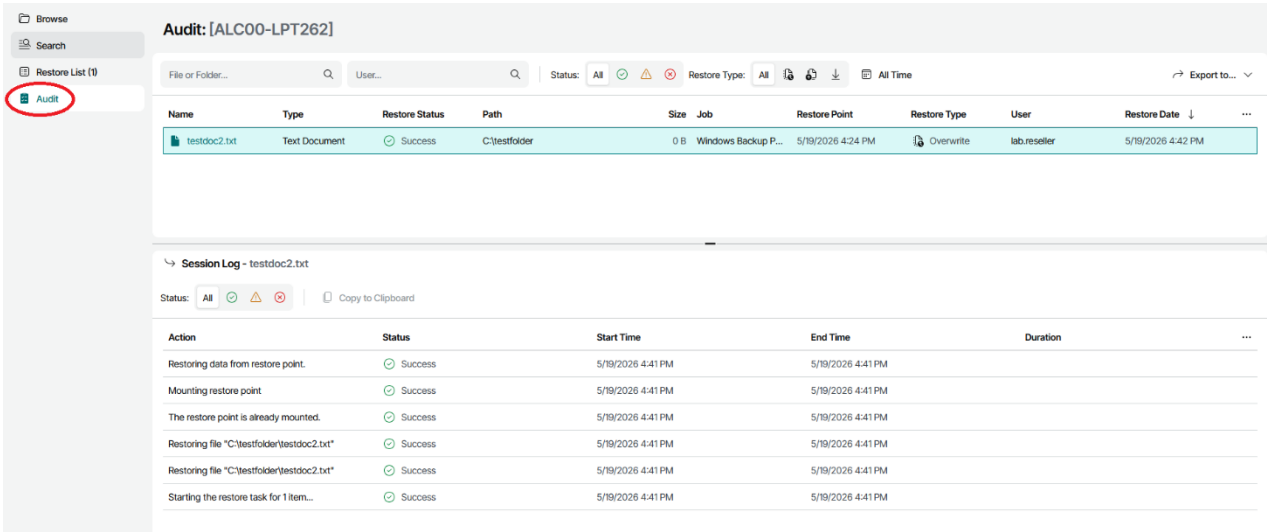
↑ Restore | ↓ Download | Stop Restore | × Remove from Restore List

| 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:



5.9 Recuperação completa da máquina

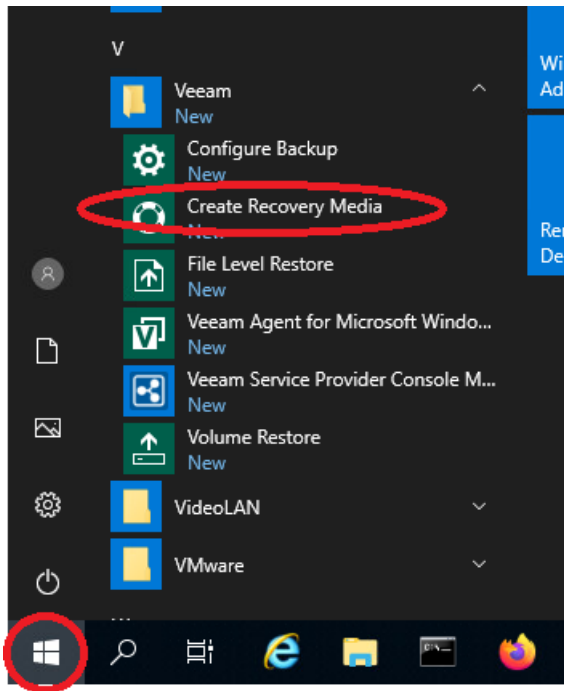
5.9.1 Criação do meio de recuperação em máquinas Windows

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

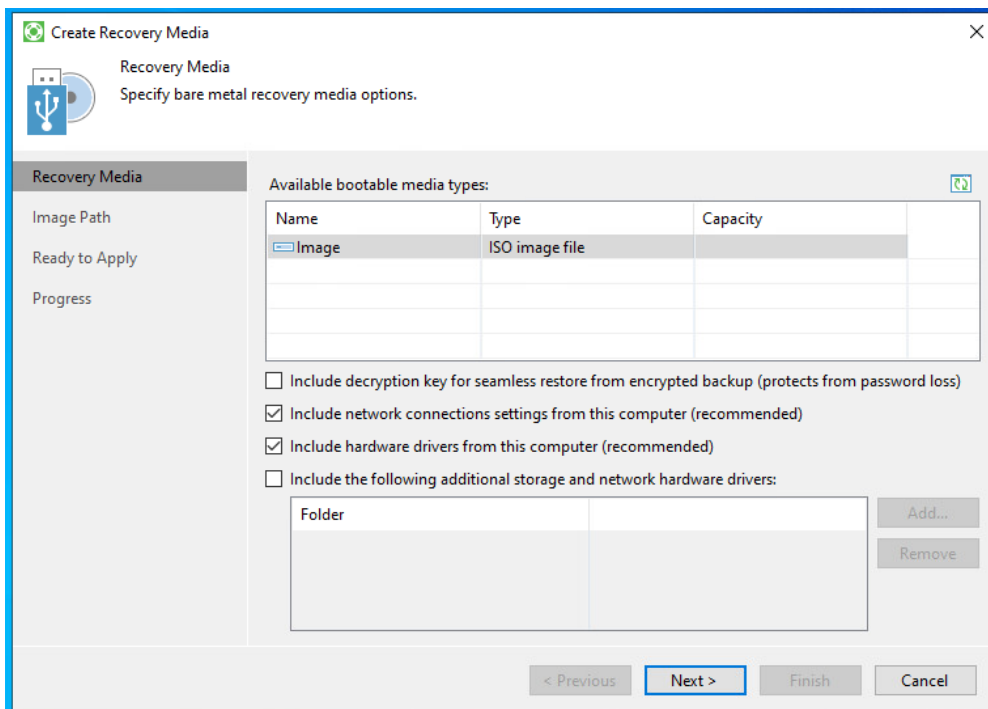
Para isso, para cada máquina passível de recuperação total, deve-se aceder à aplicação "Create Recovery Media".



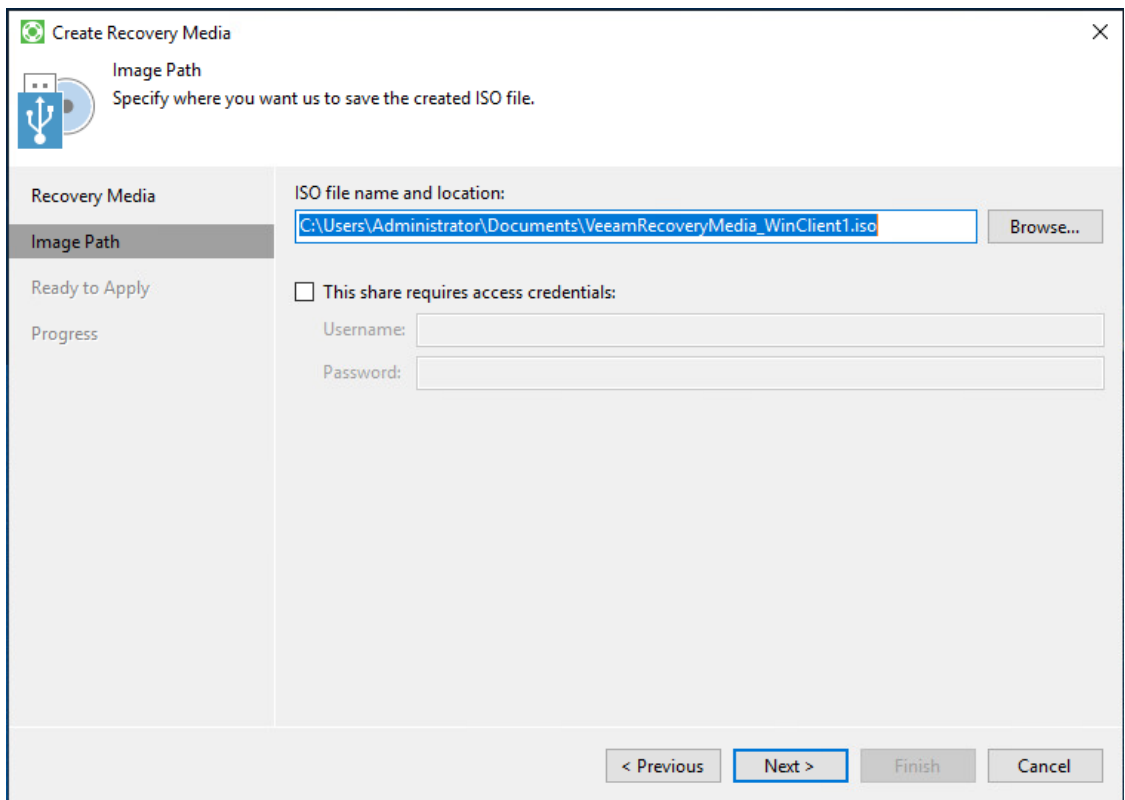
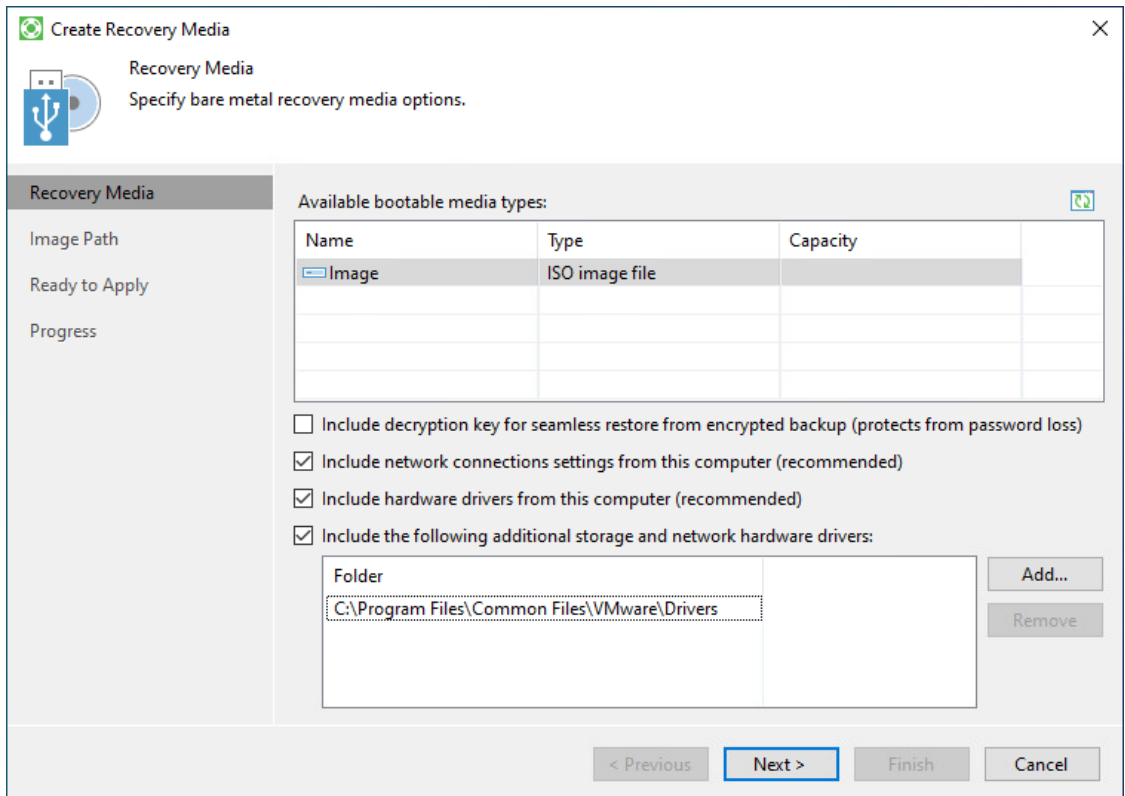
Existe um problema conhecido com *Recovery Medias* criados a partir de Windows Server 2022. O *Recovery Media* pode falhar durante o boot ou apresentar erros de certificado SSL mais à frente. Recomenda-se que se use outra versão de Windows para o criar.



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.

5.9.2 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.

5.9.3 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:

Network settings

Available networks:

No network adapters detected.
Please load a driver to continue.

Load network adapter driver OK Cancel

Hardware Drivers

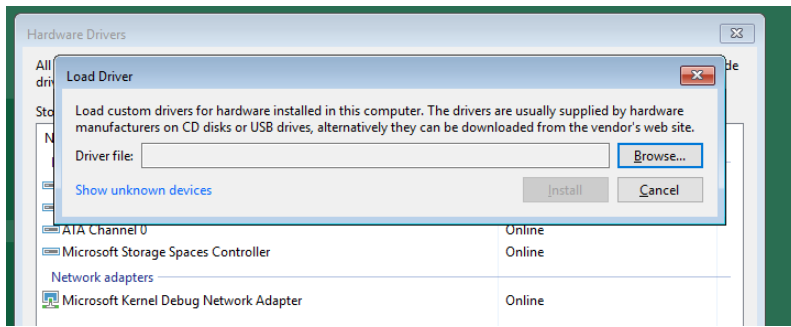
All storage and network adapters for which drivers are available are shown below. If your recovery media does not include drivers for some adapters, click Load Driver below to supply the driver manually.

Storage and network adapters:

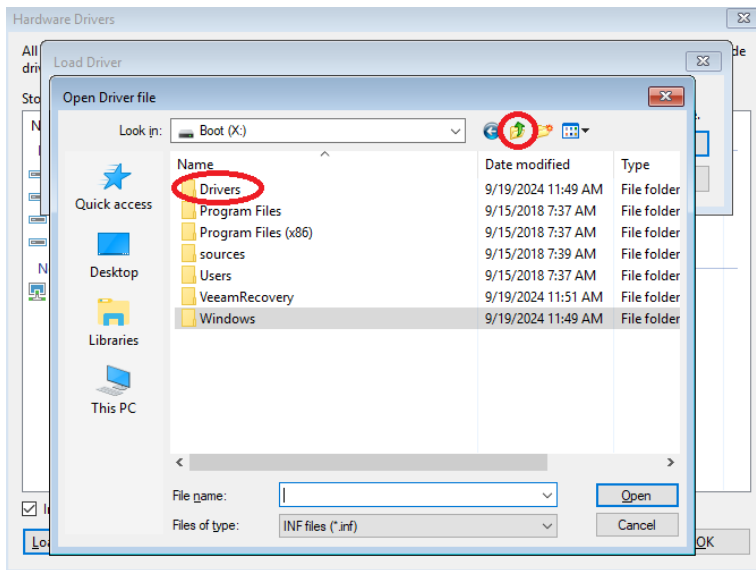
| Name | State |
|--|--------|
| Disk drives | |
| Intel(R) 823715B PCI Bus Master IDE Controller | Online |
| ATA Channel 1 | Online |
| ATA Channel 0 | Online |
| Microsoft Storage Spaces Controller | Online |
| Network adapters | |
| Microsoft Kernel Debug Network Adapter | Online |

Inject these drivers into operating system while performing bare metal recovery

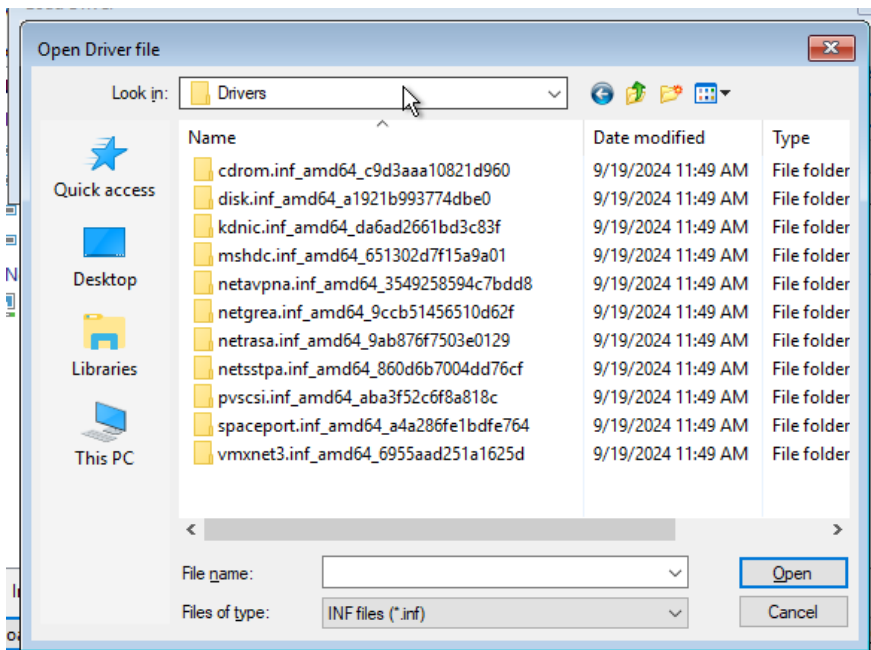
Load Driver OK



Navegar até à pasta de "Drivers":

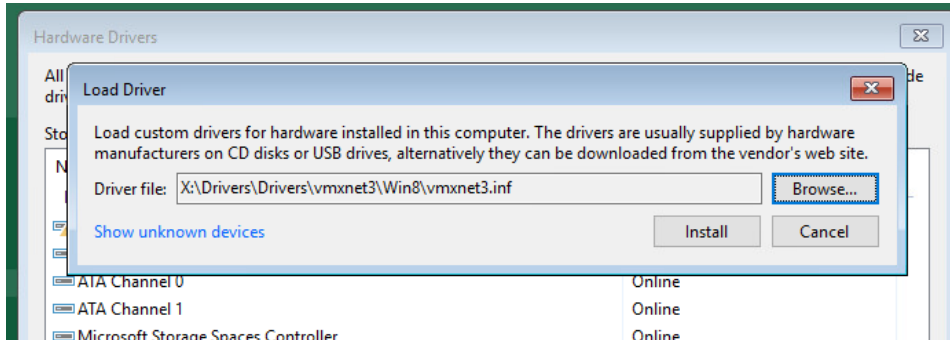


E escolher o driver em conformidade:

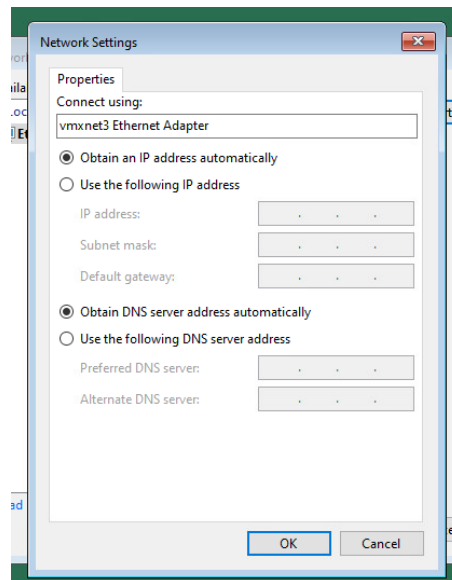
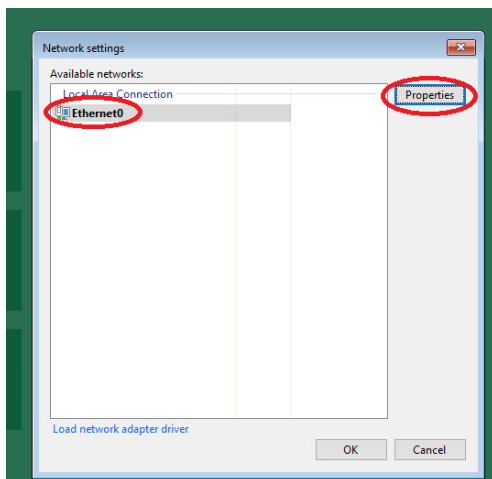




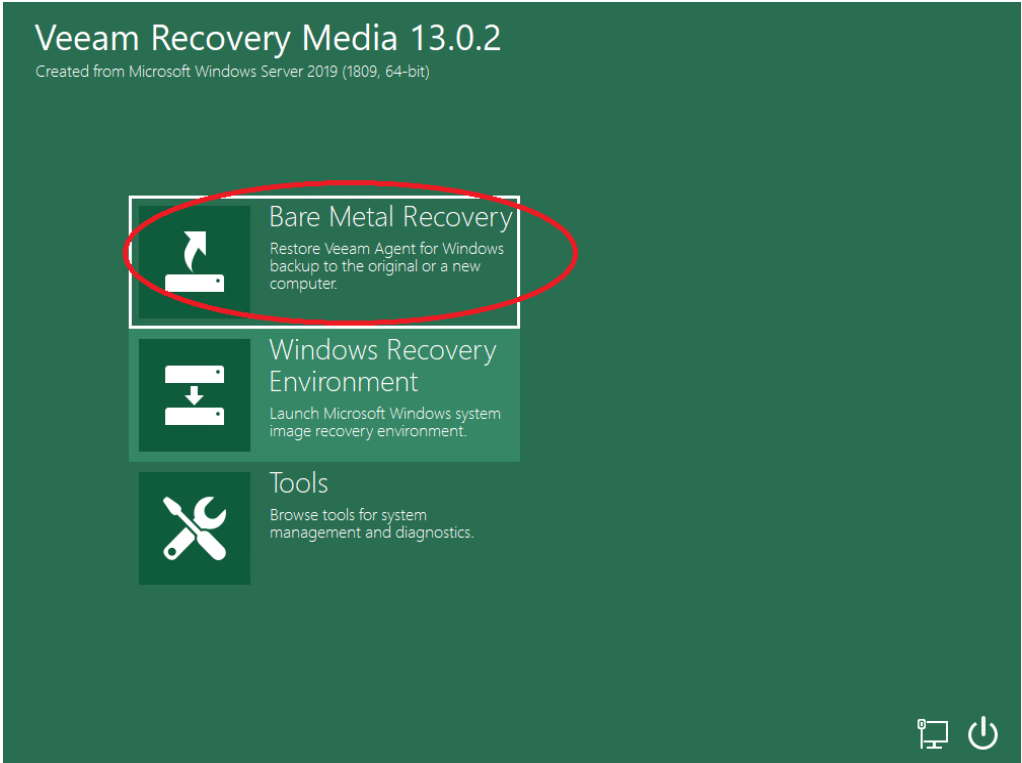
No caso de se estar a recuperar para uma máquina que não a original, é necessário criar um *Media Recovery* que inclua os drivers necessários para esta nova máquina de destino.



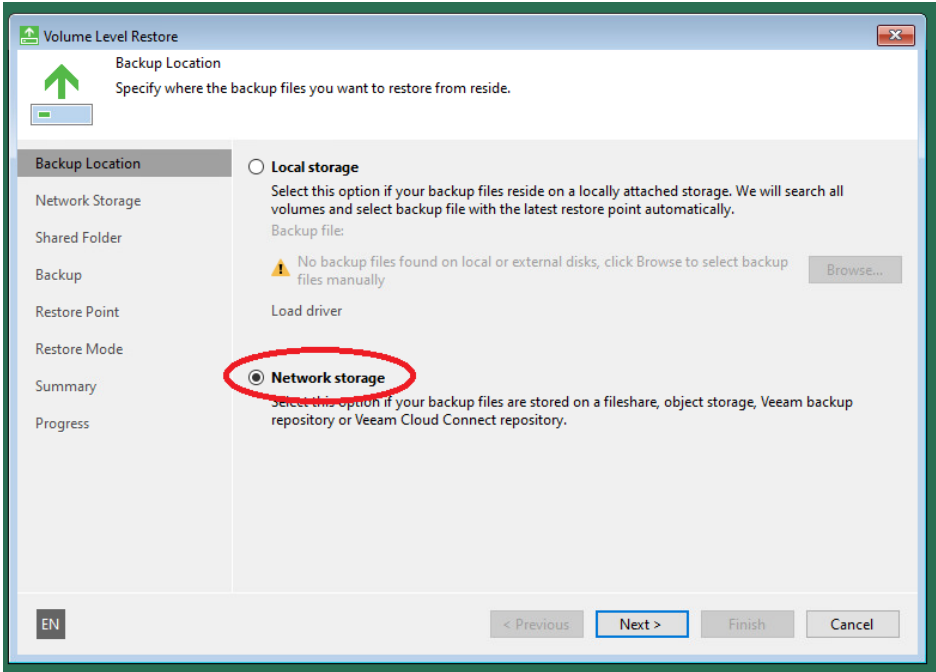
Depois do driver de rede instalado, verifica-se a configuração de rede e altera-se em conformidade:



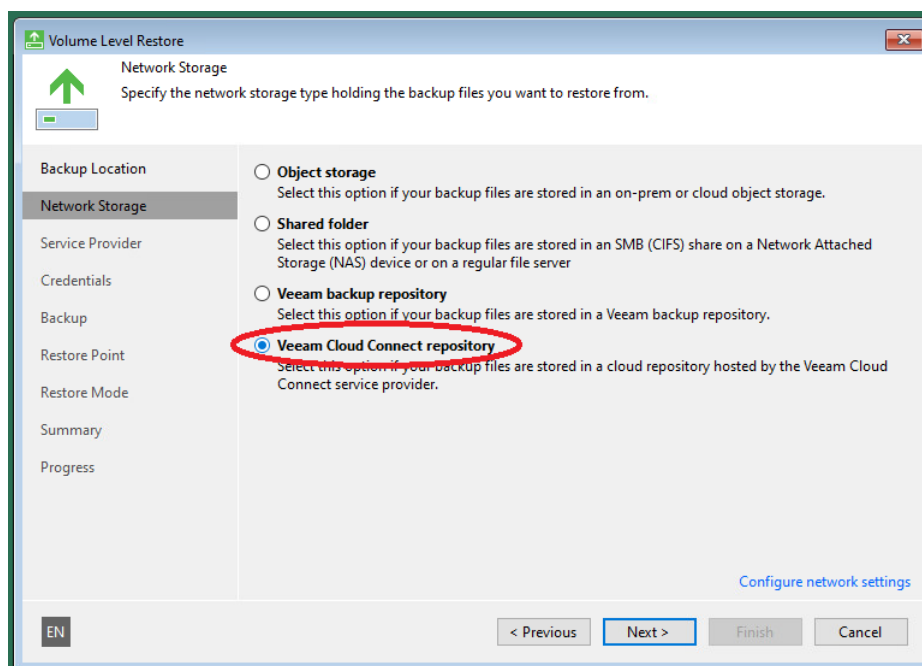
Depois de corretamente configurado, pode-se verificar que o ícone de rede não apresenta indicação de erro. Pode ainda ser necessário instalar outros drivers (por exemplo de disco/storage). Assim que todos os drivers estiverem instalados, pode-se prosseguir para a recuperação Bare Metal.



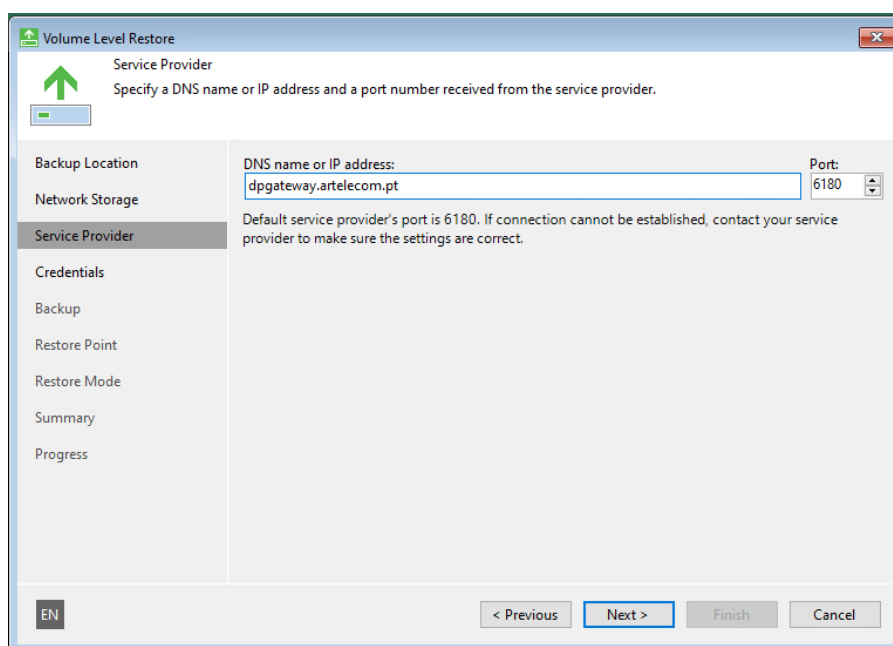
Como pretendemos recuperar a máquina com um backup do repositório da Ar, escolhemos "Network storage" como localização:



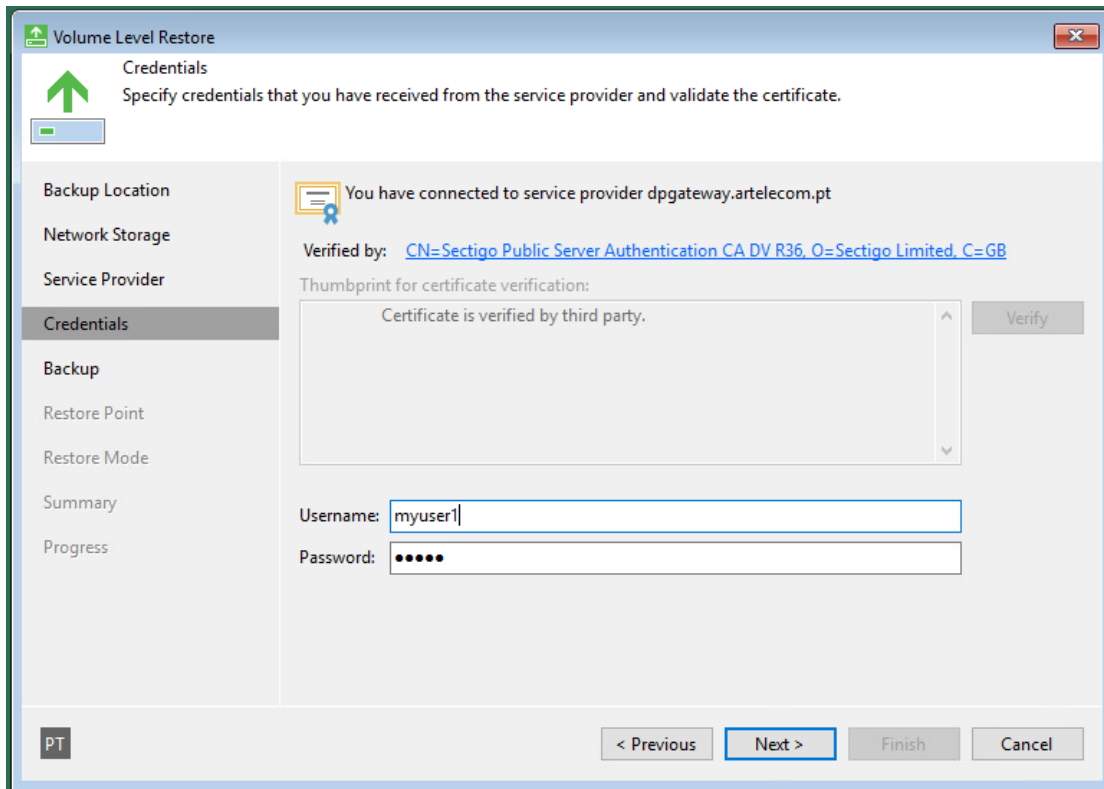
e "Veeam Cloud Connect repository"



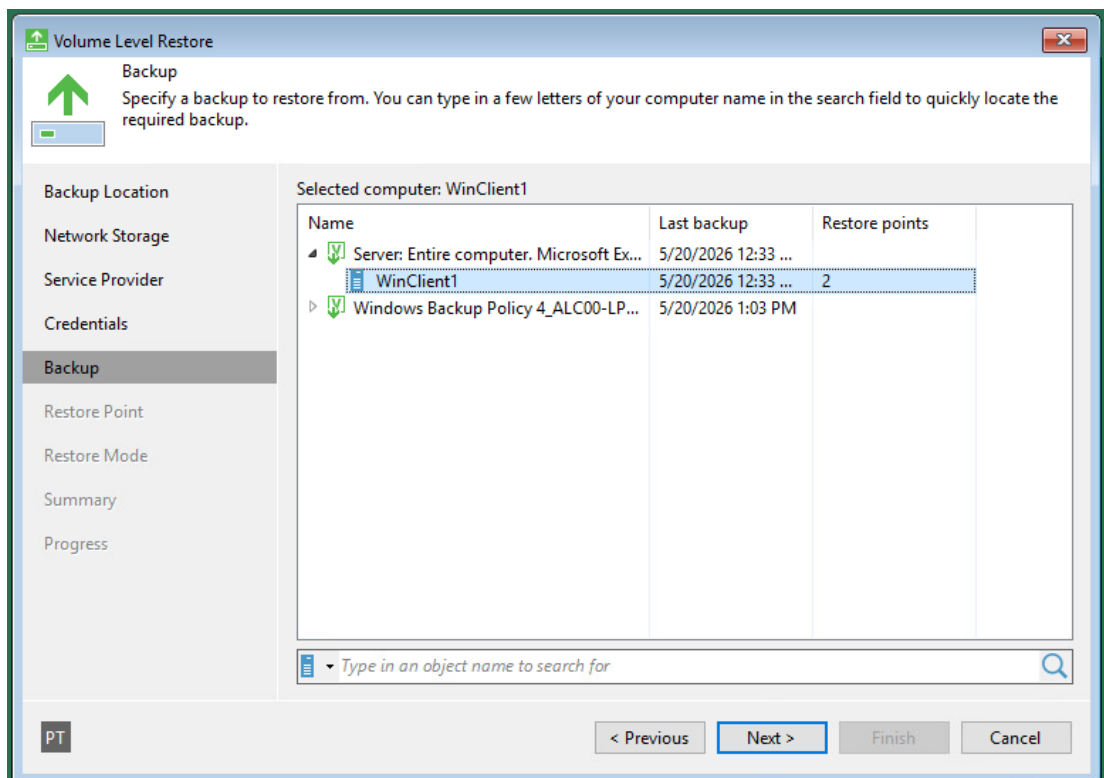
O próximo passo é introduzir o endereço da gateway da Ar que foi enviado no email de boas-vindas (por defeito usar **dpgateway.artelecom.pt** na porta **6180**):



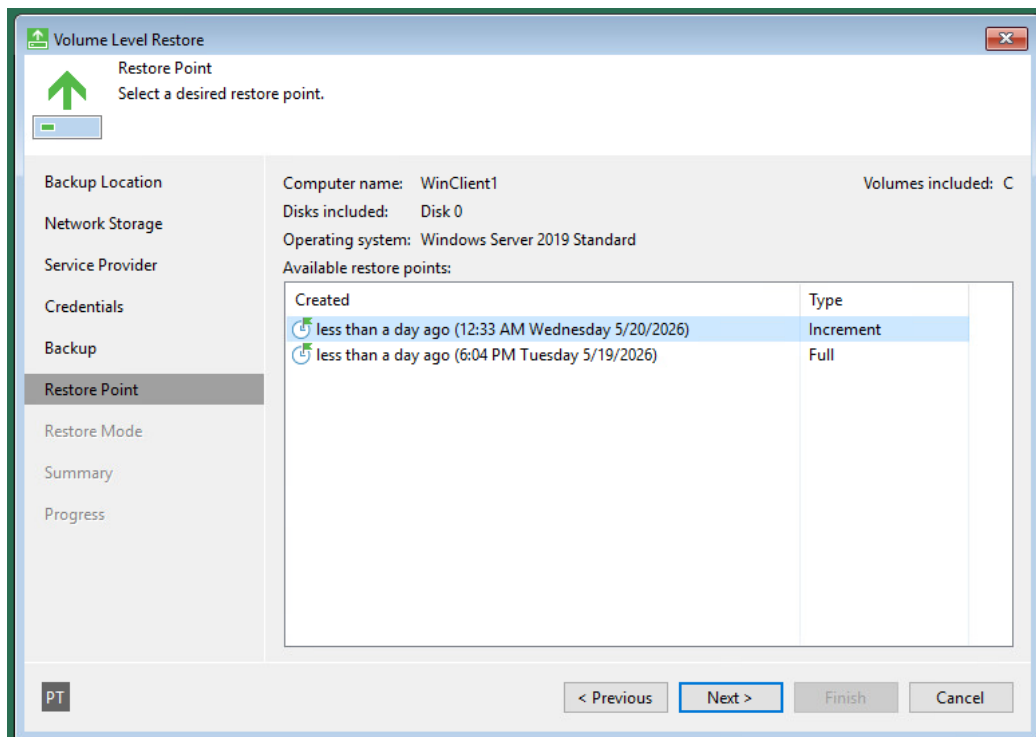
Depois de verificado o certificado SSL, é solicitada a introdução das credenciais de acesso do utilizador owner da companhia de onde se está a recuperar. Estas credenciais correspondem às que foram definidas quando se criou o tenant, como é descrito no ponto 4.2.



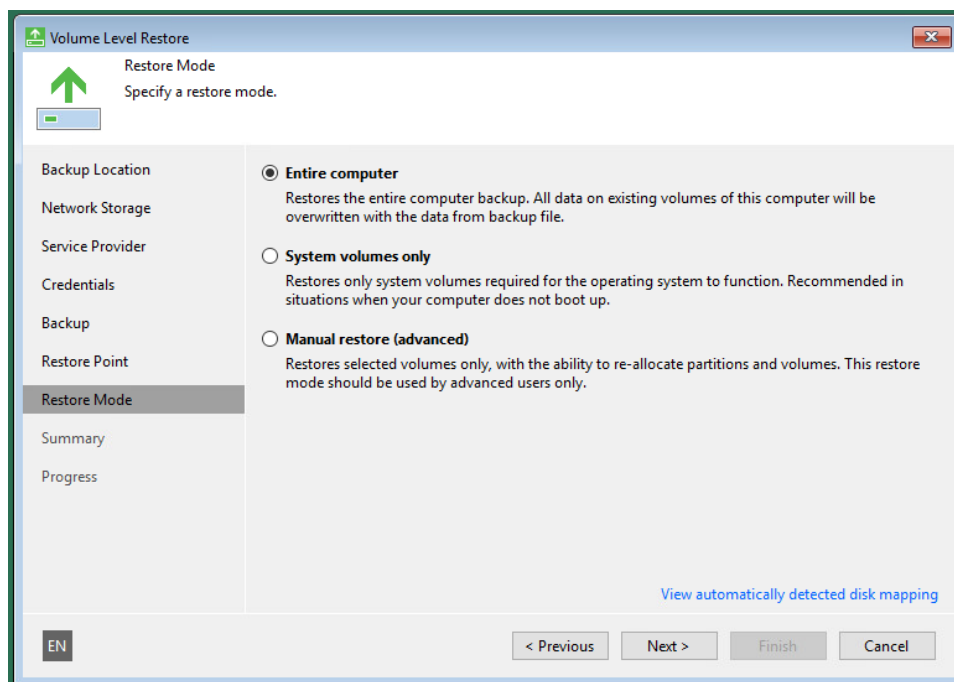
e após corretamente autenticado, podemos escolher qual o backup a recuperar:



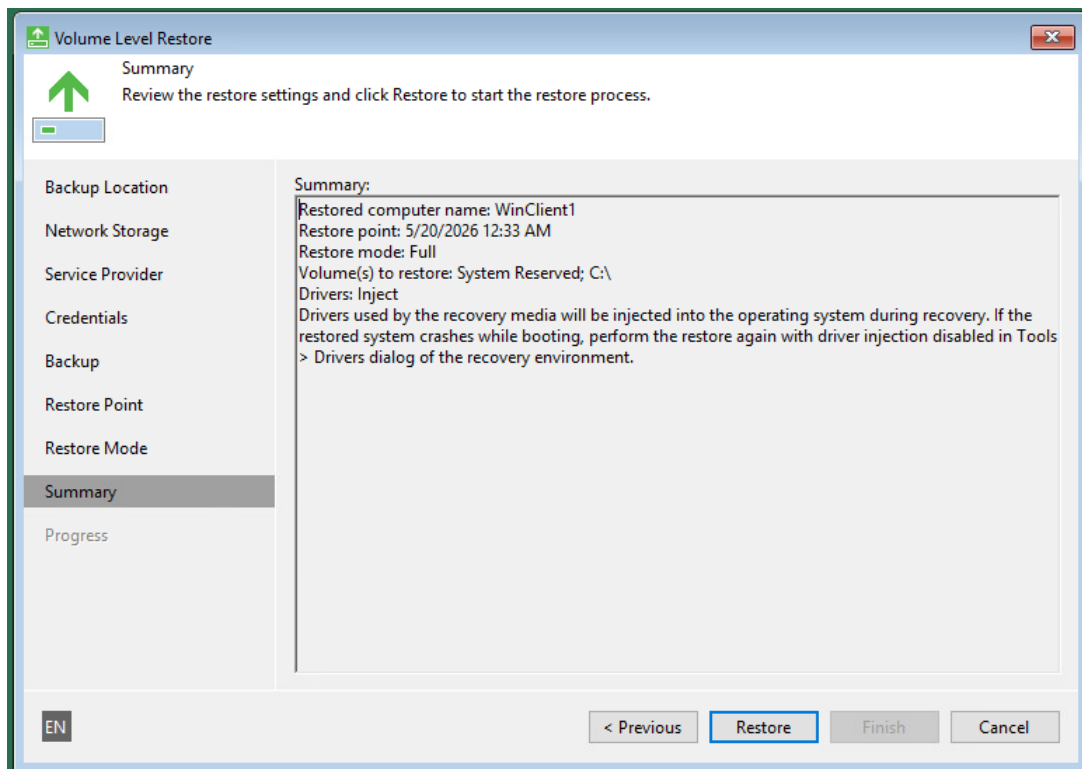
qual o ponto de restauro e avançar carregando em "Next":



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



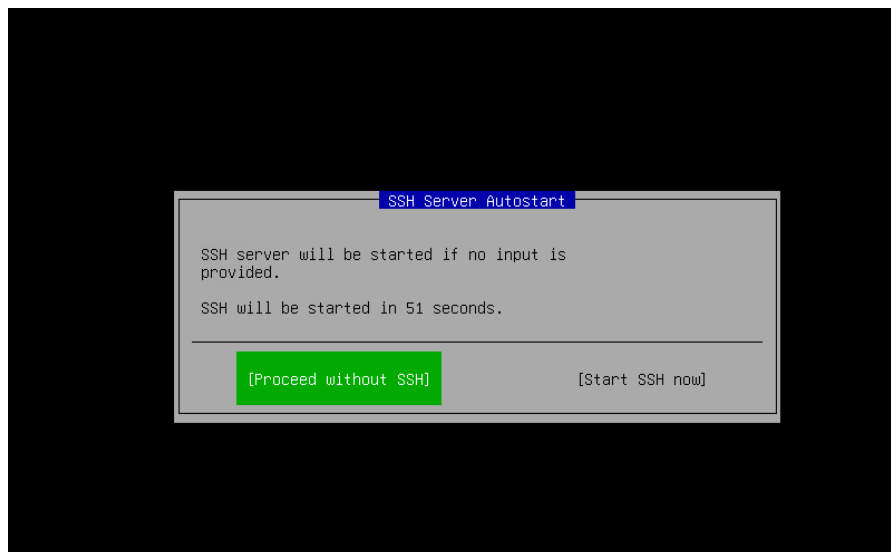
Se a máquina onde vai ser feito o restauro completo tiver partições no disco, pode ser necessário fazer o mapeamento manual das partições restauradas. Se o disco estiver limpo, o Veeam criará as partições tal como estavam na máquina original.



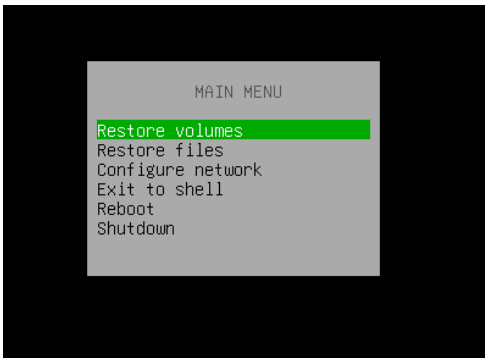
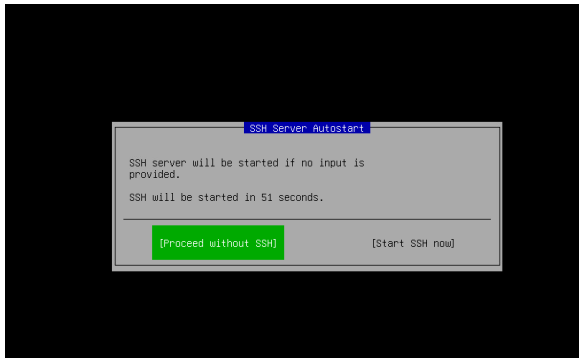
Depois do processo concluído, retirar o *Recovery Media* do boot e reiniciar a máquina.

5.9.4 Recuperação com base no Recovery Media Linux

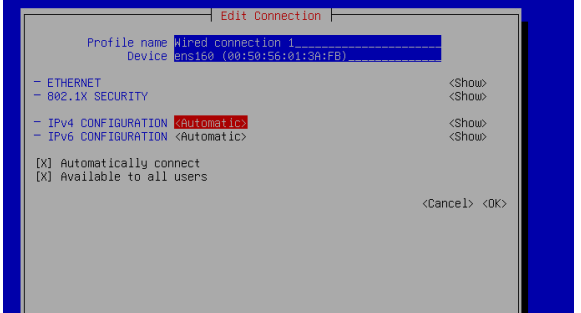
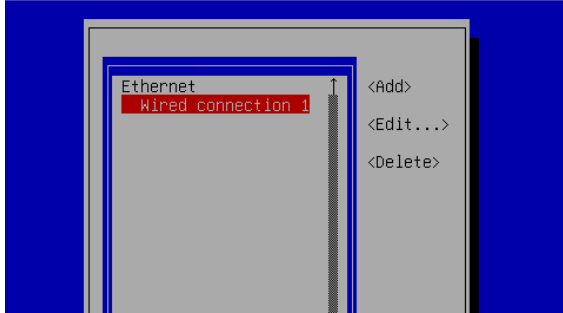
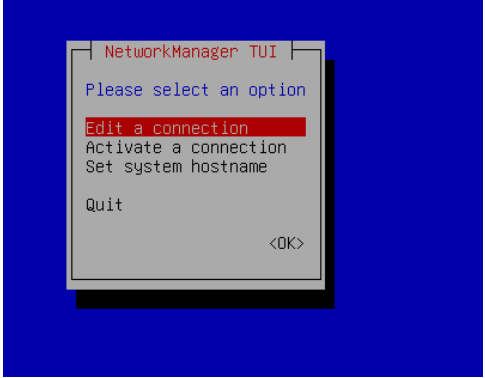
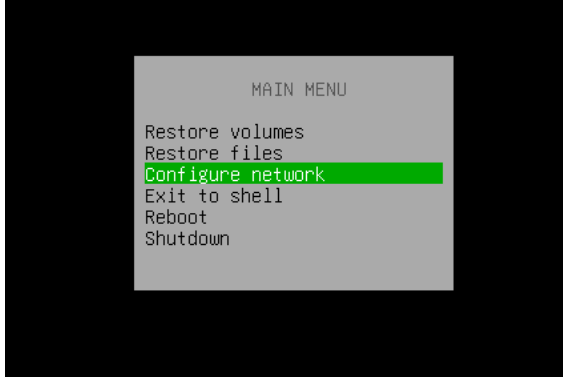
Ao fazer boot por este meio, surge um quadro dando a opção de iniciar o serviço SSH caso se pretenda fazer a recuperação remotamente.

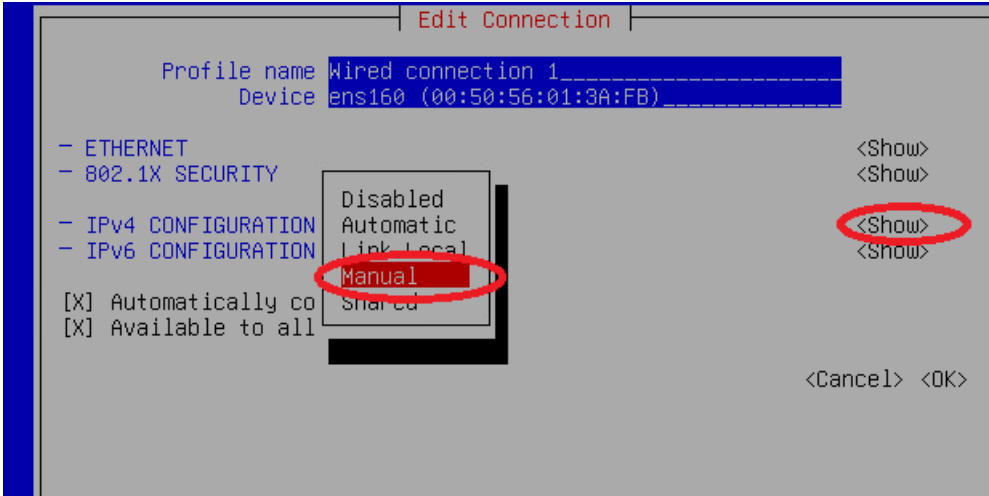


Continuando na consola, o próximo passo é aceitar os termos do licenciamento seguindo-se o menu de recuperação:

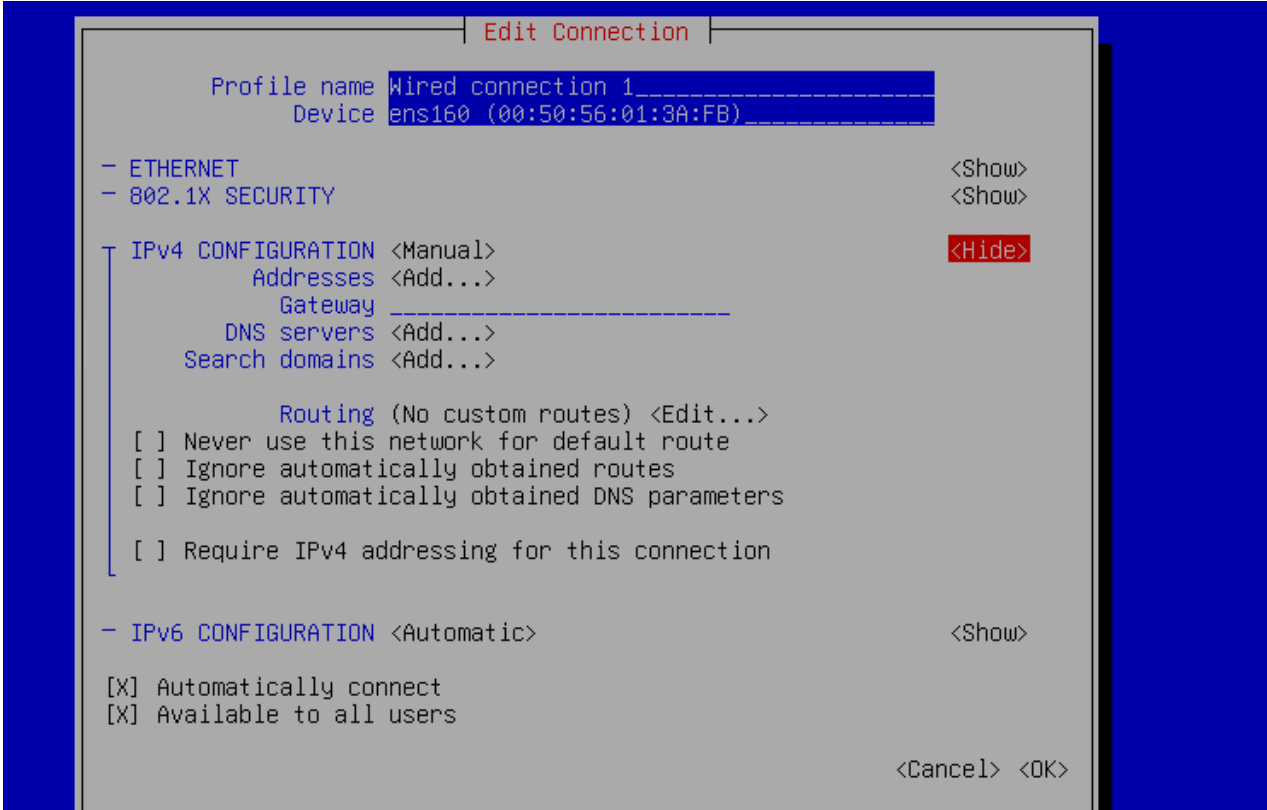


Para recuperar a máquina a partir do repositório da Ar é necessário garantir que a conectividade de rede esteja ativa e, portanto, é necessário configurar a rede:

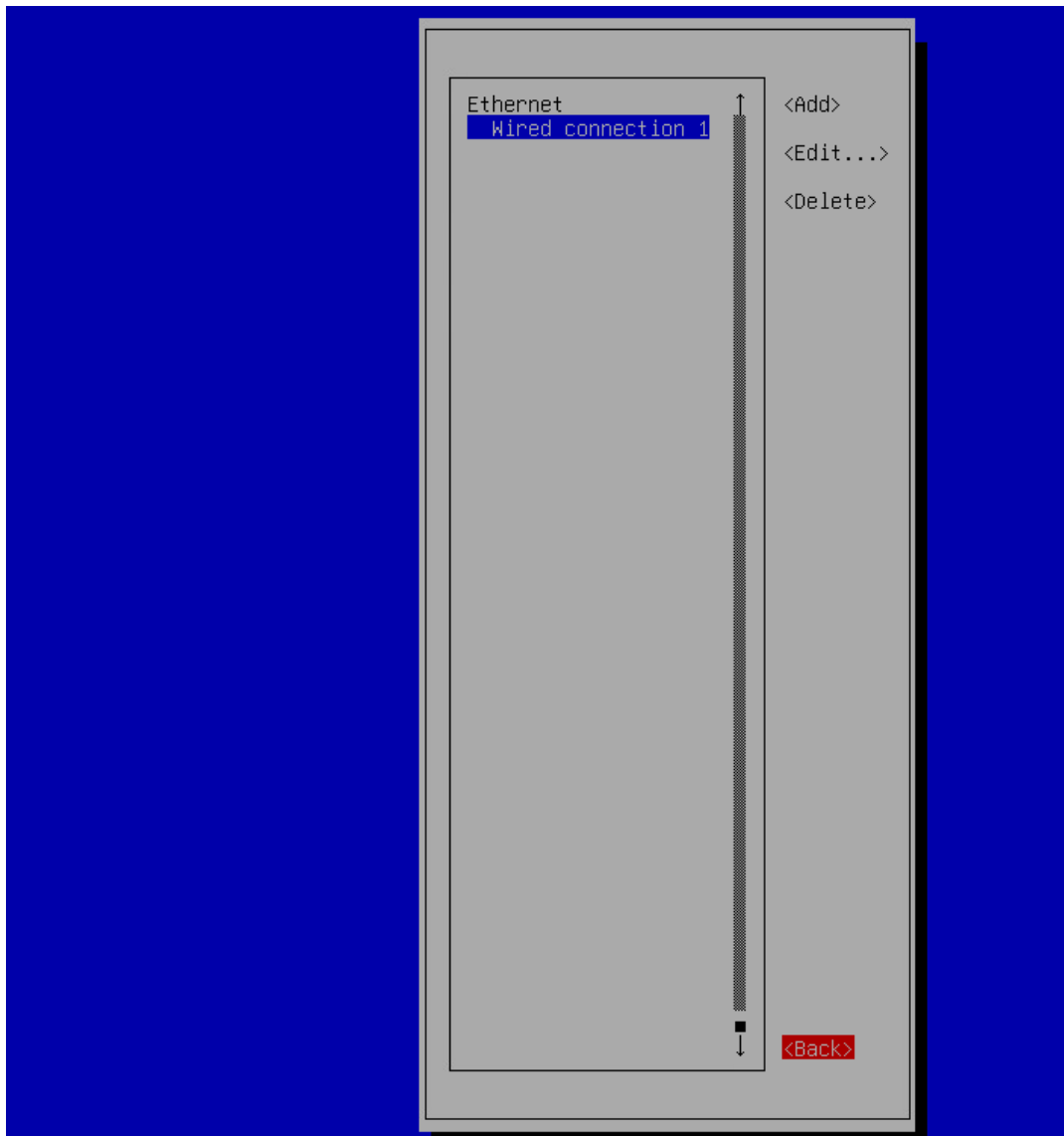




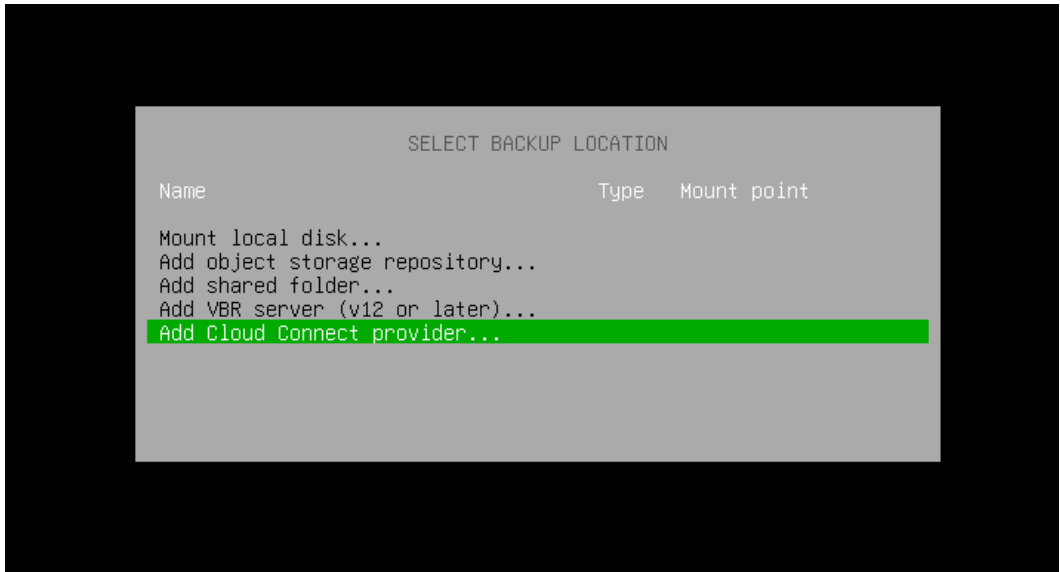
Configurar a rede em conformidade e fazer <OK>:



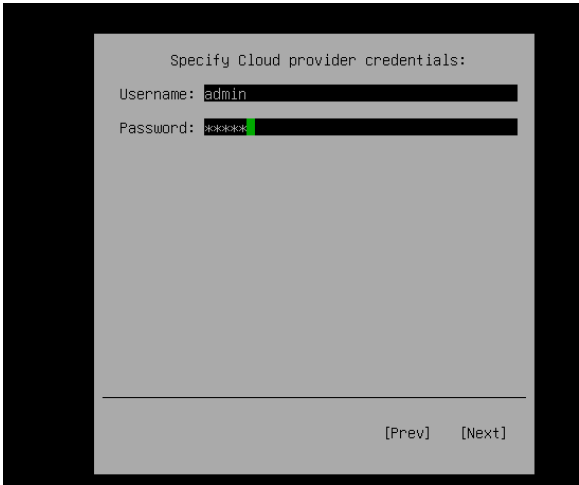
No quadro que vai aparecer fazer <Back>



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 Boas-Vindas e introduzir as credenciais que foram definidas quando se criou o tenant, como é descrito no ponto 4.2:



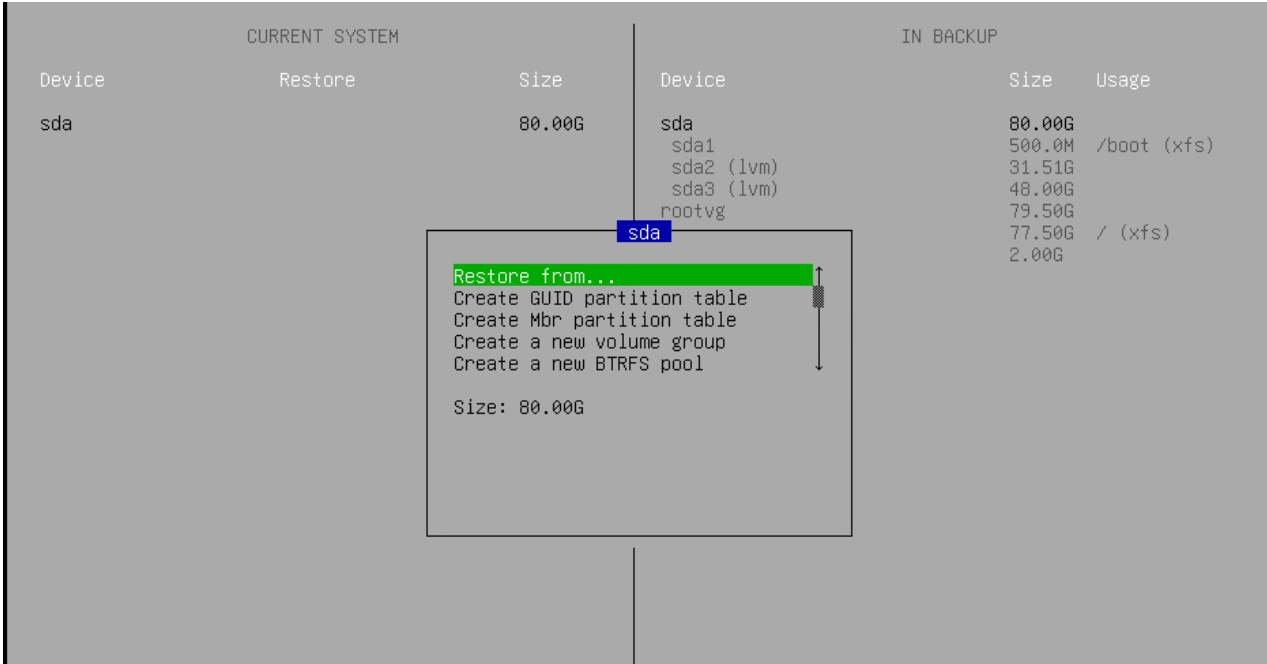
A partir daqui é possível escolher o backup e qual o ponto de restauro a recuperar:

| 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 |

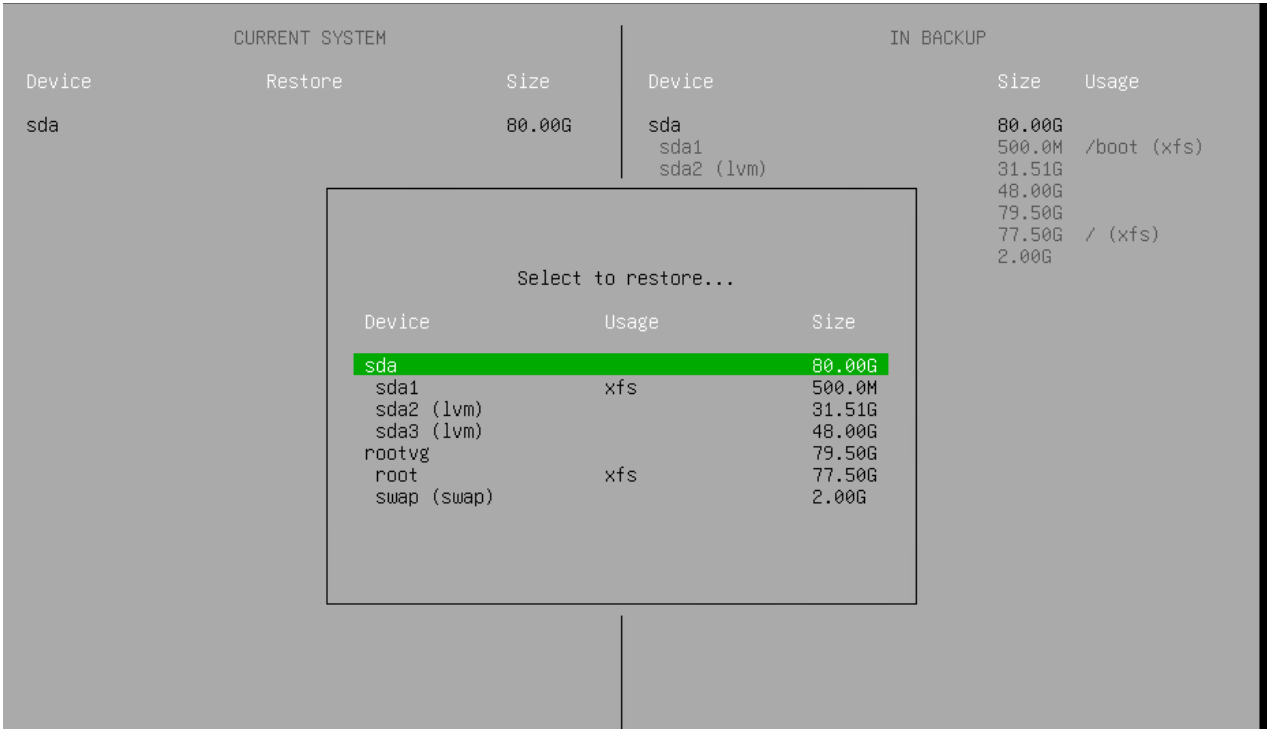
E quais os volumes:

| 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 | |

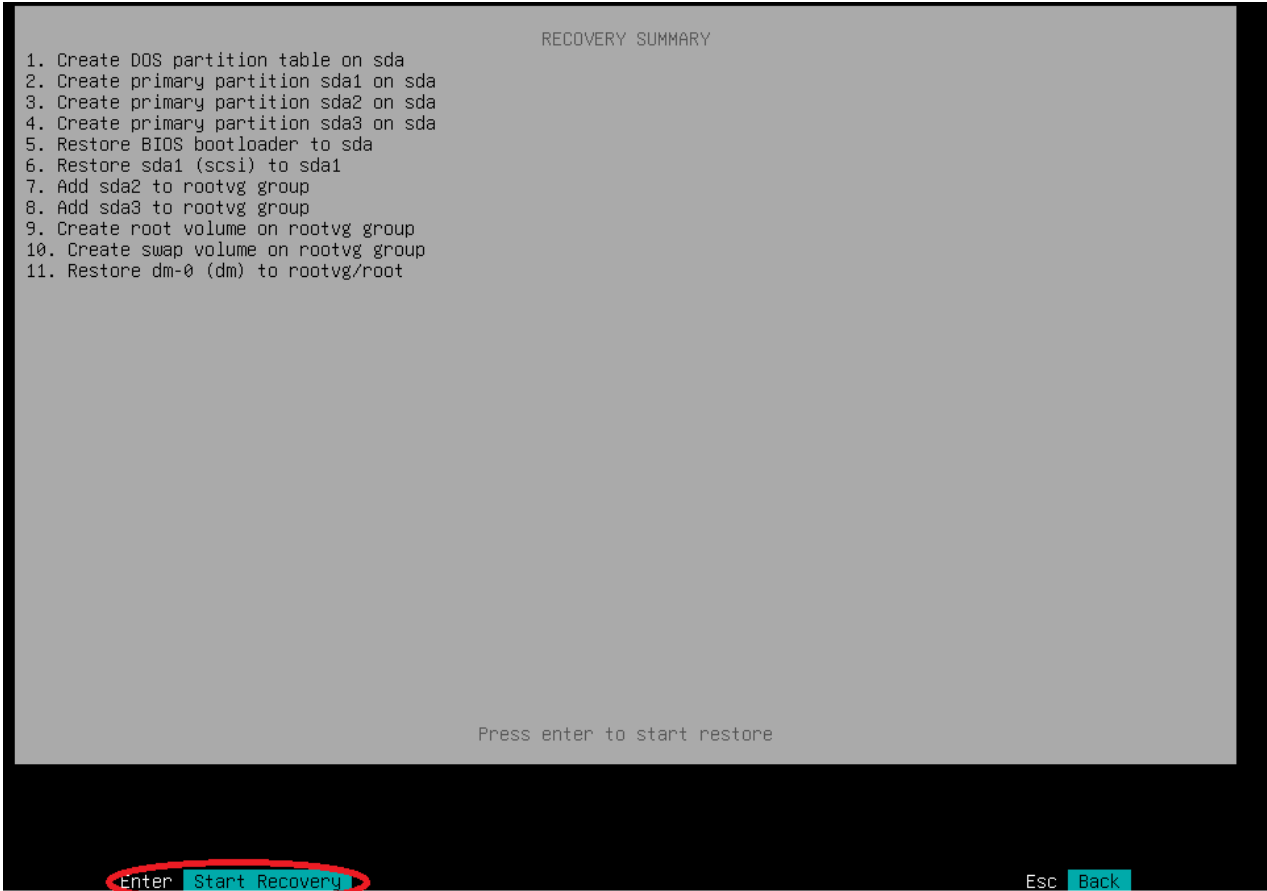
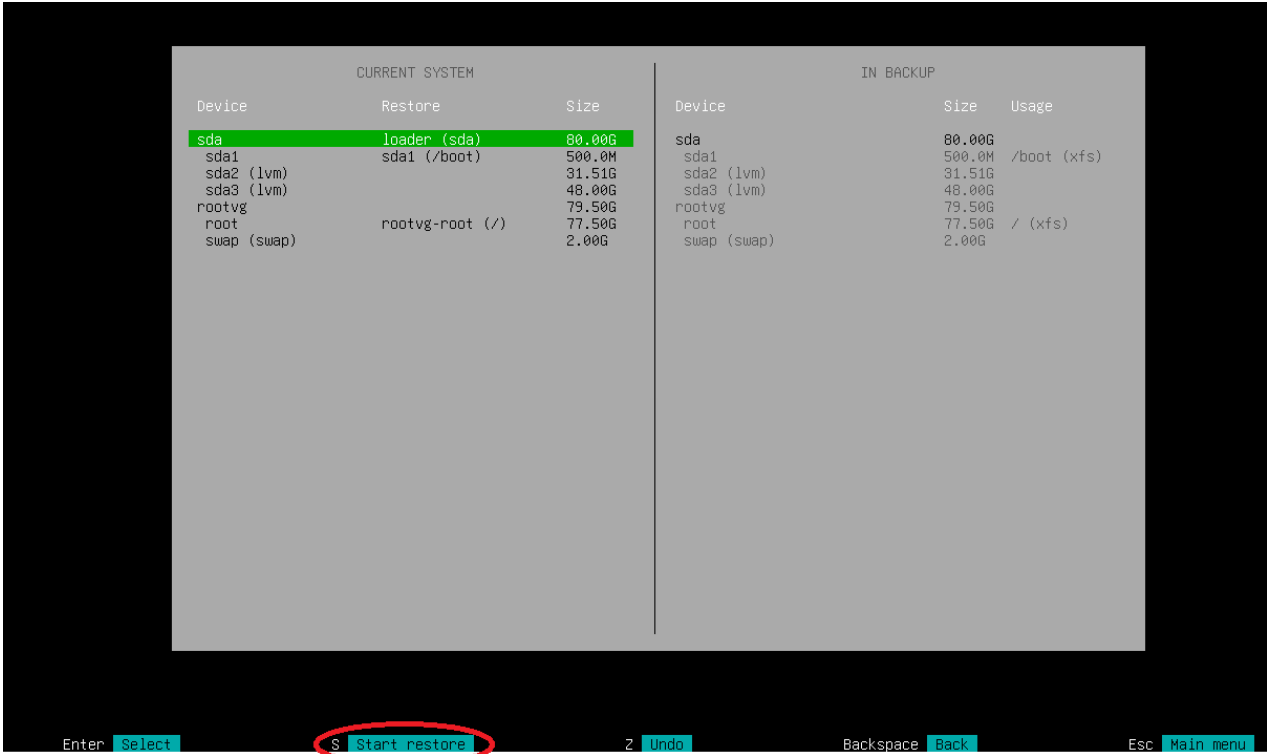
Selecionar o dispositivo pretendido (neste caso das) e escolher "Restore from...":



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
13:53:15  rootvg-root restored 77.5 GB at 21.4 MB/s  00:00:12
14:55:03  sdal restored 500 MB at 17.1 MB/s          01:01:48
14:55:32  Restoring bootloader on /dev/sda          00:00:29
14:55:39  Processing finished at 2024-09-17 14:55:39 UTC  00:00:01
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

```

5.10 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.