

	PROCEDIMENTO	
	ROTINAS DE BACKUP – CLOUD E FITAS	Identificação: PRO-TI-006
		Versão: 01

1. OBJETIVO

Este documento tem por objetivo orientar os colaboradores nas atividades de suporte as áreas da Belliz.

2. RESPONSABILIDADES

A execução e monitoramento das atividades descritas neste procedimento não de inteira responsabilidade da equipe de TI.

3. DESCRIÇÃO

3.1 ROTINAS DE BACKUPS – CLOUD E FITA

As políticas de backup foram definidas para mantermos um padrão na cópia das informações da empresa, garantindo a segurança da informação e total sigilo.

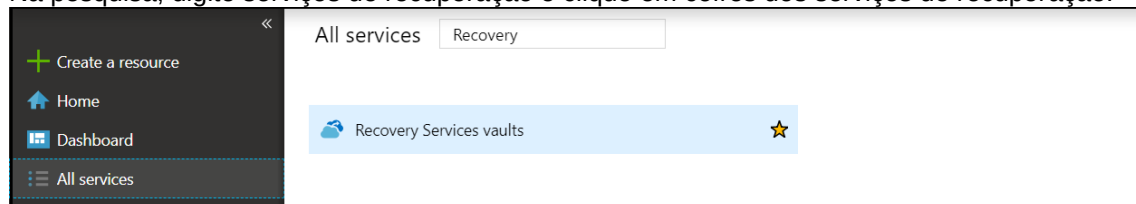
Esse padrão também visa assegurar que todas as informações necessárias ao funcionamento da empresa estejam disponíveis, por meio de restauração, em caso de perda acidental, roubo de equipamentos, incêndios, alagamentos e/ou desastres naturais.

3.1.1 CLOUD - CRIAR UM COFRE DOS SERVIÇOS DE RECUPERAÇÃO

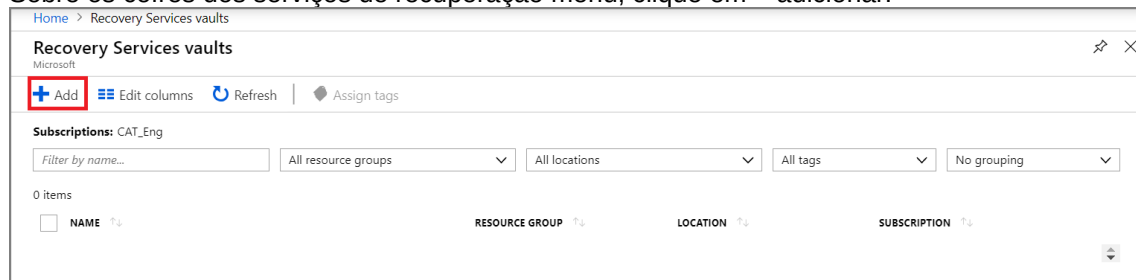
recuperação criados ao longo do tempo e contém a política de backup aplicada ao backup de máquinas. Crie um cofre da seguinte maneira:

Entre no Portal do Azure usando sua assinatura do Azure.

Na pesquisa, digite serviços de recuperação e clique em cofres dos serviços de recuperação.



Sobre os cofres dos serviços de recuperação menu, clique em + adicionar.

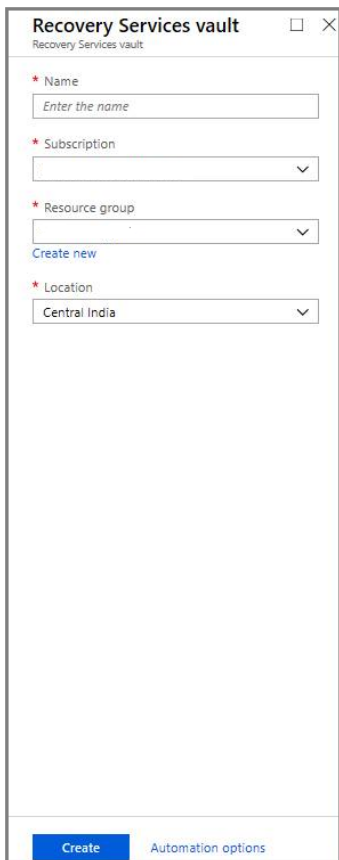


Em Nome, insira um nome amigável para identificar o cofre.

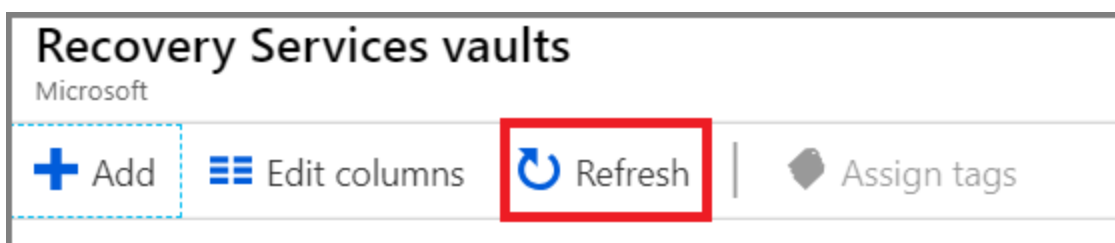
- O nome deve ser exclusivo para a assinatura do Azure.
- Ele pode conter caracteres de 2 a 50.
- Ele deve começar com uma letra e pode conter apenas letras, números e hifens.

Selecione a assinatura do Azure, grupo de recursos e região geográfica em que o cofre deve ser criado. Dados de backup são enviados para o cofre. Em seguida, clique em Criar.

	PROCEDIMENTO	
	ROTINAS DE BACKUP – CLOUD E FITAS	Identificação: PRO-TI-006
		Versão: 01



Pode levar algum tempo para que o cofre seja criado. Monitore as notificações de status na área superior direita do portal. Se após alguns minutos, você não vir o cofre, clique em **“Refresh”**



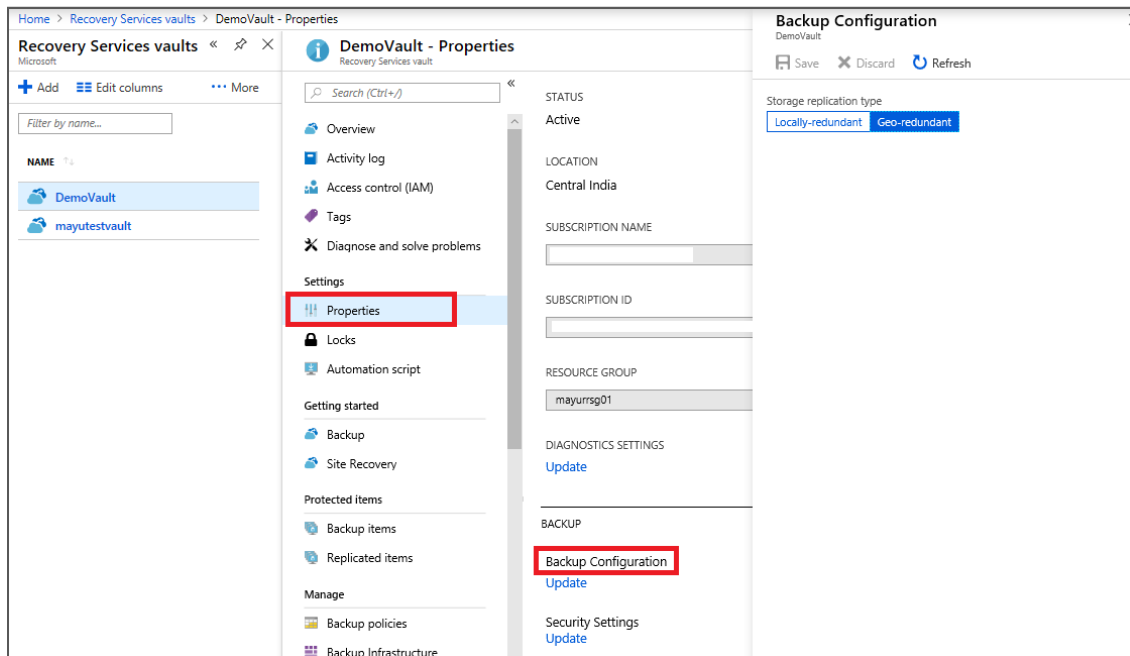
3.1.2 DEFINIR REDUNDÂNCIA DE ARMAZENAMENTO

O Backup do Azure controla automaticamente o armazenamento para o cofre. Você precisa especificar como esse armazenamento é replicado.

Na folha Cofres dos Serviços de Recuperação, clique no novo cofre. Sob o as configurações seção, clique em propriedades.

Nas propriedades, em configuração de Backup, clique em atualização.

Selecione o tipo de replicação de armazenamento e, em seguida, clique em salvar.



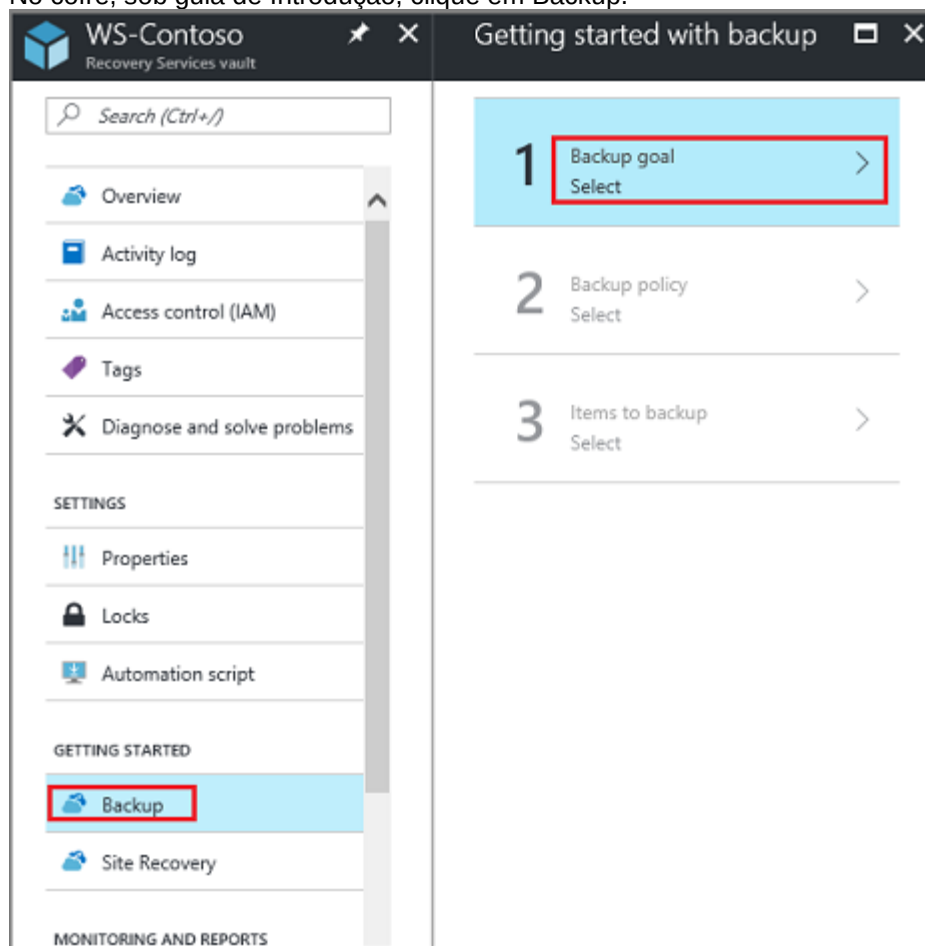
Recomendamos que se você estiver usando o Azure como um ponto de extremidade do armazenamento de backup principal, continue a usar o padrão georedundante configuração. Se você não usar o Azure como um ponto de extremidade de armazenamento de backup principal, escolha localmente redundante, que reduz os custos de armazenamento do Azure. Saiba mais sobre geográfica e local redundância.

3.1.3 BAIXE O AGENTE DE MARS

Baixe o agente MARS para instalação em computadores que você deseja fazer backup. Se você já tiver instalado o agente em computadores, verifique se que você estiver executando a versão mais recente. A versão mais recente está disponível no portal ou usando um download direto.

	PROCEDIMENTO	
	ROTINAS DE BACKUP – CLOUD E FITAS	Identificação: PRO-TI-006
		Versão: 01

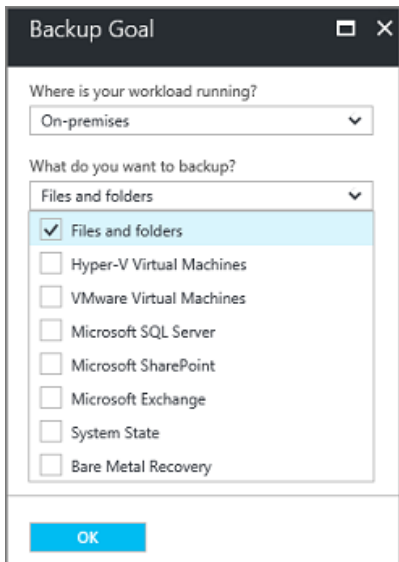
No cofre, sob guia de Introdução, clique em Backup.



No campo “**Onde sua carga de trabalho é executada?**” selecione “**local**”. Você deve selecionar essa opção, mesmo se você quiser instalar o agente de MARS em uma VM do Azure.

No campo “**O que fazer você deseja fazer backup?**” selecione **arquivos e pastas e/ou estado do sistema**. Há várias outras opções disponíveis, mas eles só têm suporte se você estiver executando um servidor de backup secundário. Clique em **preparar a infraestrutura**.

	PROCEDIMENTO	
	ROTINAS DE BACKUP – CLOUD E FITAS	Identificação: PRO-TI-006
		Versão: 01



Backup Goal

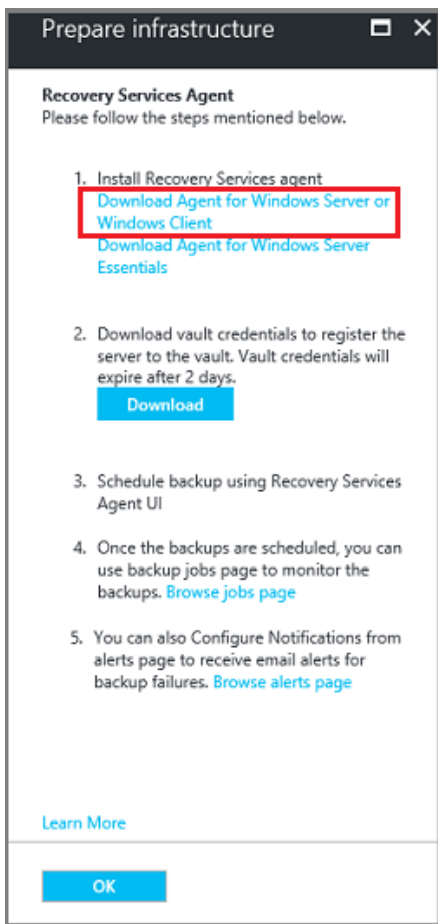
Where is your workload running?
On-premises

What do you want to backup?
Files and folders

- ☒ Files and folders
- ☐ Hyper-V Virtual Machines
- ☐ VMware Virtual Machines
- ☐ Microsoft SQL Server
- ☐ Microsoft SharePoint
- ☐ Microsoft Exchange
- ☐ System State
- ☐ Bare Metal Recovery

OK

No preparar infraestrutura, em agente dos Recovery Services instalar, baixe o agente de MARS.



Prepare infrastructure

Recovery Services Agent
Please follow the steps mentioned below.

1. Install Recovery Services agent
[Download Agent for Windows Server or Windows Client](#)
[Download Agent for Windows Server Essentials](#)
2. Download vault credentials to register the server to the vault. Vault credentials will expire after 2 days.
[Download](#)
3. Schedule backup using Recovery Services Agent UI
4. Once the backups are scheduled, you can use backup jobs page to monitor the backups. [Browse jobs page](#)
5. You can also Configure Notifications from alerts page to receive email alerts for backup failures. [Browse alerts page](#)

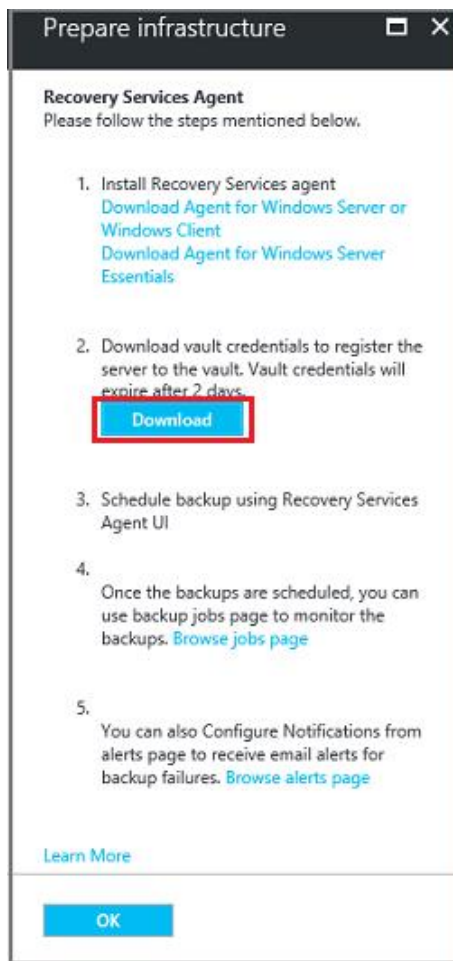
[Learn More](#)

OK

	PROCEDIMENTO	
	ROTINAS DE BACKUP – CLOUD E FITAS	Identificação: PRO-TI-006
		Versão: 01

Clique em **Salvar** no menu pop-up de download. Por padrão, o arquivo **MARSagentinstaller.exe** será salvo em sua pasta Downloads.

Agora, verifique já download ou usando o agente de serviços de recuperação mais recente, em seguida, baixe as credenciais do cofre.



Clique em Salvar. O arquivo é baixado para a pasta de Download. Você não pode abrir o arquivo de credenciais do cofre.

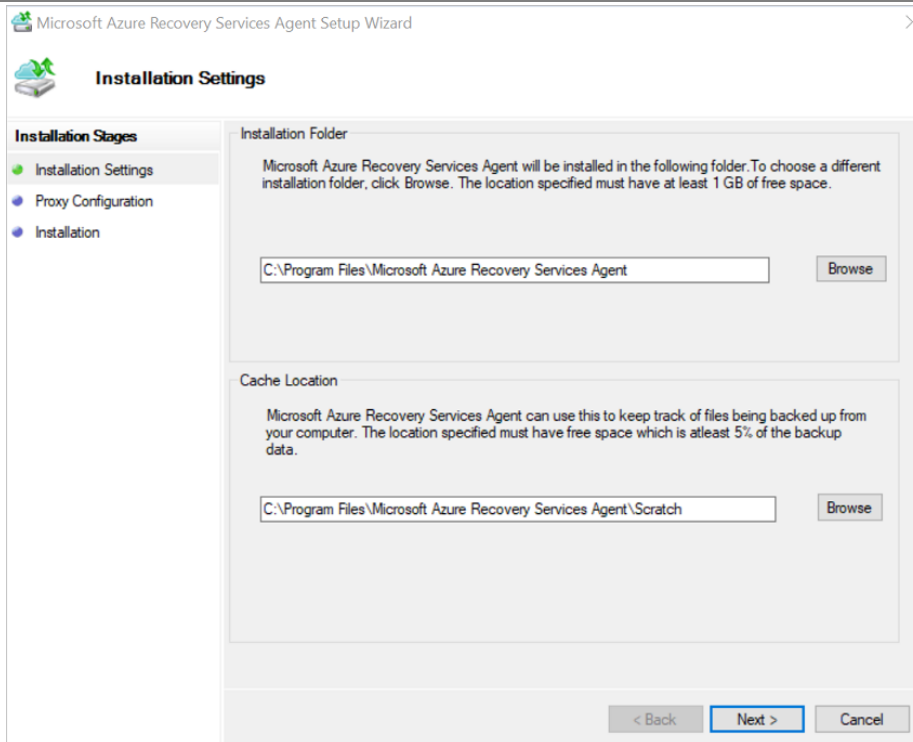
3.1.4 INSTALAR E REGISTRAR O AGENTE

Execute o MARSagentinstaller.exe arquivo nos computadores que você deseja fazer backup.

No Assistente de instalação do agente MARS > configurações de instalação, especifique onde você deseja instalar o agente e um local a ser usado para o cache. Em seguida, clique em Próximo.

- O Backup do Azure usa o cache para armazenar os instantâneos de dados antes de enviá-los para o Azure.
- O local do cache deve ter espaço livre igual a pelo menos 5% do tamanho dos dados que você pode fazer backup.

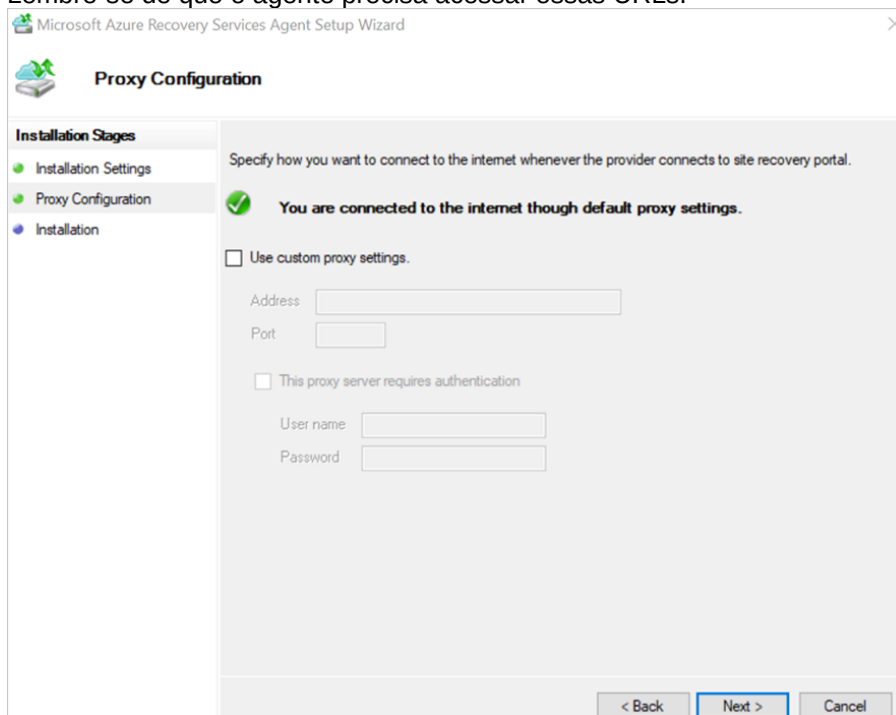
	PROCEDIMENTO	
	ROTINAS DE BACKUP – CLOUD E FITAS	Identificação: PRO-TI-006
		Versão: 01



The screenshot shows the 'Installation Settings' window of the Microsoft Azure Recovery Services Agent Setup Wizard. On the left, the 'Installation Stages' list includes 'Installation Settings' (selected), 'Proxy Configuration', and 'Installation'. The main area is divided into two sections: 'Installation Folder' and 'Cache Location'. The 'Installation Folder' section contains a text box with the path 'C:\Program Files\Microsoft Azure Recovery Services Agent' and a 'Browse' button. The 'Cache Location' section contains a text box with the path 'C:\Program Files\Microsoft Azure Recovery Services Agent\Scratch' and a 'Browse' button. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

Na configuração de Proxy, especifique como o agente em execução no computador do Windows se conectará à internet. Em seguida, clique em Próximo.

- Se você estiver usando um personalizado proxy especificar as configurações de proxy e as credenciais se necessário.
- Lembre-se de que o agente precisa acessar essas URLs.

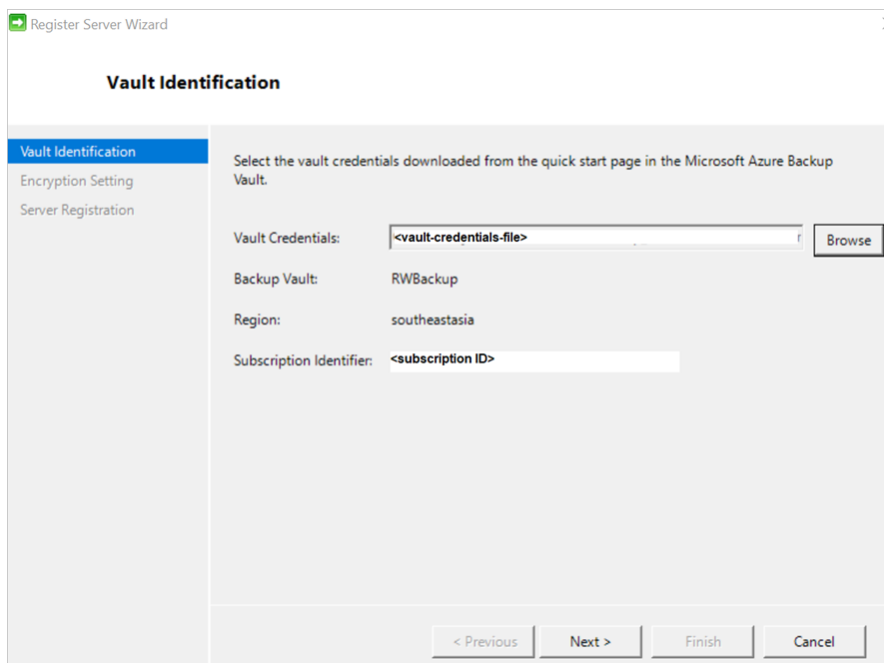


The screenshot shows the 'Proxy Configuration' window of the Microsoft Azure Recovery Services Agent Setup Wizard. On the left, the 'Installation Stages' list includes 'Installation Settings', 'Proxy Configuration' (selected), and 'Installation'. The main area has a heading 'Specify how you want to connect to the internet whenever the provider connects to site recovery portal.' Below this, there is a green checkmark icon and the text 'You are connected to the internet though default proxy settings.' There is an unchecked checkbox labeled 'Use custom proxy settings.' Below this checkbox are input fields for 'Address' and 'Port'. Further down, there is another unchecked checkbox labeled 'This proxy server requires authentication', followed by input fields for 'User name' and 'Password'. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

	PROCEDIMENTO	
	ROTINAS DE BACKUP – CLOUD E FITAS	Identificação: PRO-TI-006
		Versão: 01

Na instalação revisar a verificação de pré-requisitos e, em seguida, clique em instalar. Depois que o agente está instalado, clique em prosseguir com o registro.

No Assistente para registrar servidor > identificação do cofre, navegue e selecione o arquivo de credenciais que você baixou. Em seguida, clique em Próximo.



Na configuração de criptografia, especifique uma frase secreta que será usada para criptografar e descriptografar backups para a máquina.

- Salve a senha de criptografia em um local seguro.
- Se você perder ou esquecer a senha, a Microsoft não poderá ajudar a recuperar os dados de backup. Salve o arquivo em um local seguro. Você precisará dele para restaurar um backup.

Clique em concluir. Agora, o agente está instalado e seu computador está registrado no cofre. Você está pronto para configurar e agendar o backup.

3.1.5 CRIAR UMA POLÍTICA DE BACKUP

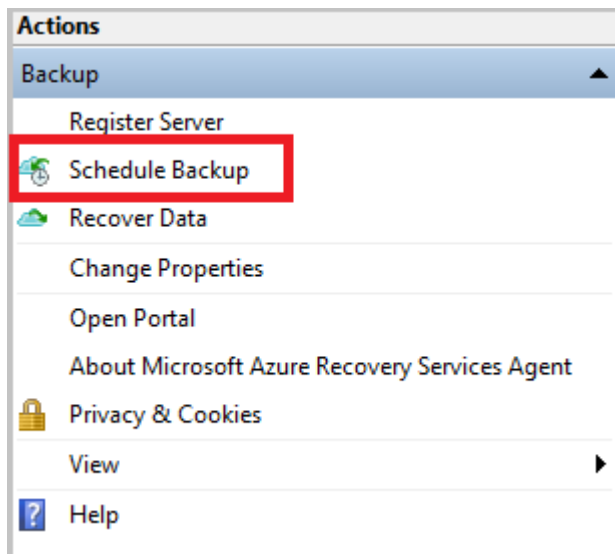
A política de backup especifica quando tirar instantâneos dos dados para criar pontos de recuperação e por quanto tempo manter os pontos de recuperação.

- Você configurar uma política de backup usando o agente do MARS.
- O Backup do Azure não automaticamente considera horário de verão (DST). Isso poderia causar alguma discrepância entre o tempo real e o horário de backup agendado. Crie uma política da seguinte maneira:

Em cada computador, abra o agente do MARS. Você pode localizá-lo pesquisando no seu computador por Backup do Microsoft Azure.

Nas ações, clique em agendar Backup.

	PROCEDIMENTO	
	ROTINAS DE BACKUP – CLOUD E FITAS	Identificação: PRO-TI-006
		Versão: 01



No Assistente de agendamento de Backup > **guia de Introdução**, clique em **próxima**.

No item “**selecionar itens para Backup**”, clique em “**Adicionar itens**”.

Na selecionar itens, selecione o que você deseja fazer backup. Em seguida, clique em OK.

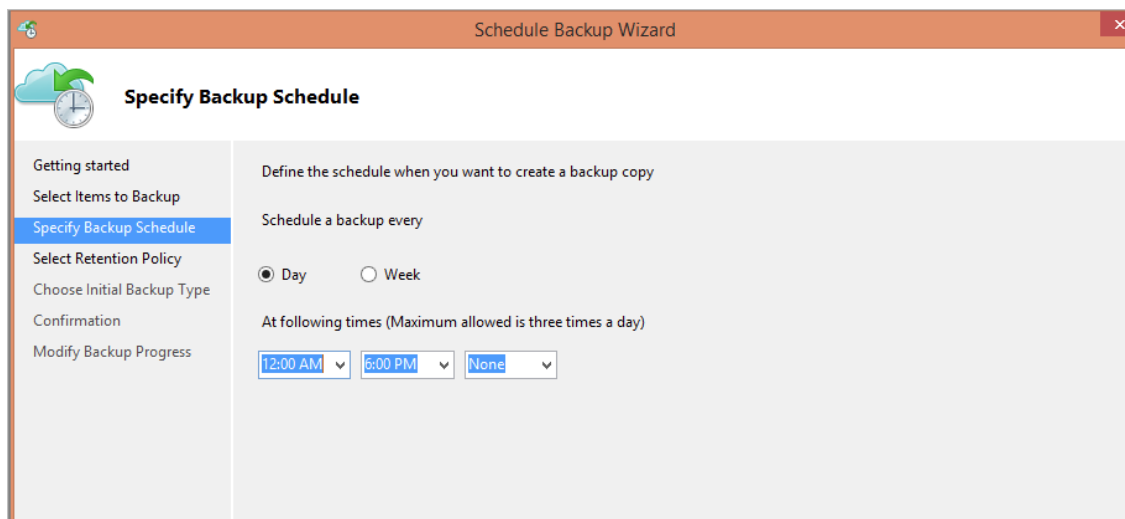
Na selecionar itens para Backup, clique em próxima.

Na especificar agendamento de Backup, especifique quando você deseja fazer backups diários ou semanais.

Em seguida, clique em Próximo.

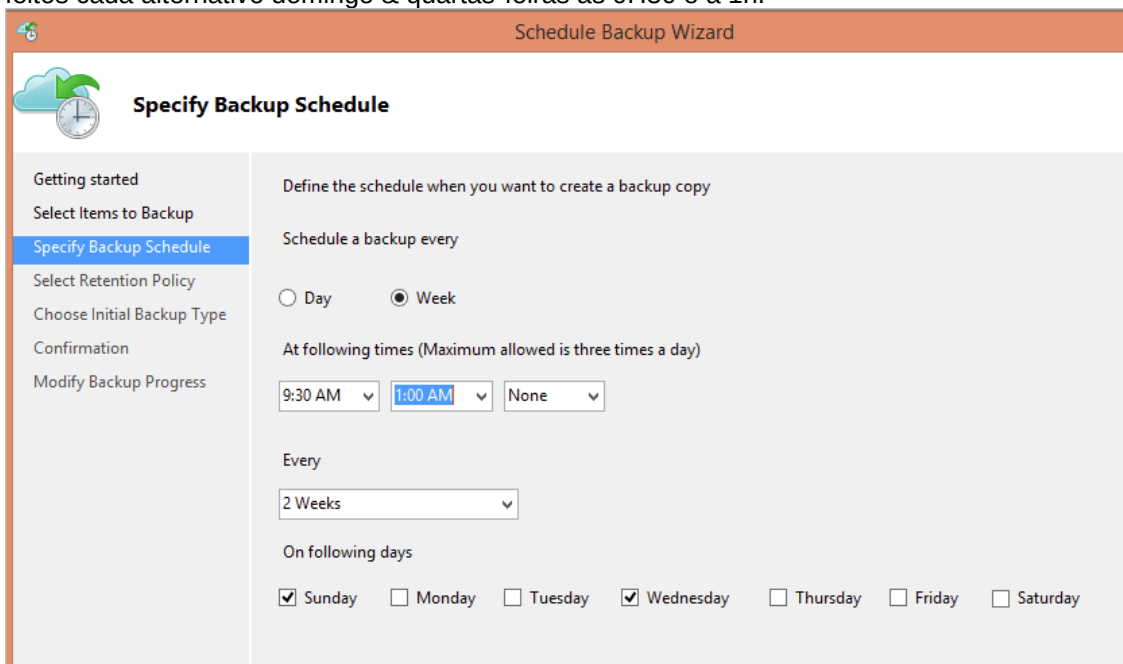
- Um ponto de recuperação é criado quando é feito um backup.
- O número de pontos de recuperação criados em seu ambiente depende do seu agendamento de backup.

Você pode agendar backups diários, até três vezes por dia. Por exemplo, a captura de tela mostra dois backups diários, uma à meia-noite e um às 18h.



	PROCEDIMENTO	
	ROTINAS DE BACKUP – CLOUD E FITAS	Identificação: PRO-TI-006
		Versão: 01

Você também pode executar backups semanais. Por exemplo, a captura de tela mostra os backups feitos cada alternativo domingo & quartas-feiras às 9H30 e à 1h.



Sobre o Selecionar política de retenção, especifique como você pode armazenar cópias históricas de seus dados. Em seguida, clique em Próximo.

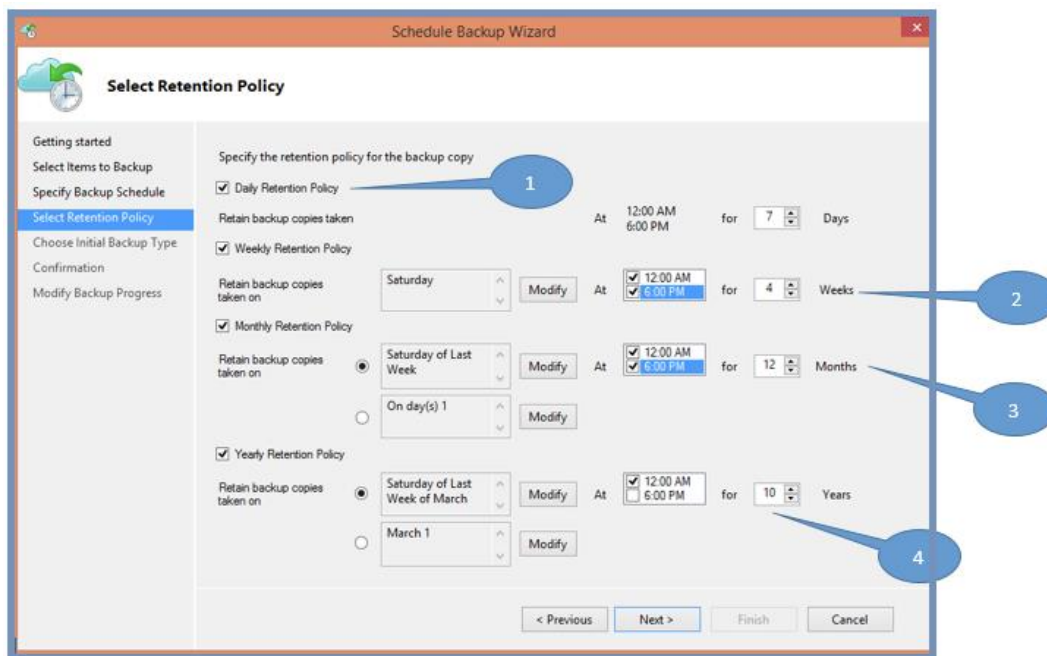
Configurações de retenção especificam quais pontos de recuperação devem ser armazenados e por quanto tempo deve ser armazenado.

Por exemplo, quando você define uma configuração de retenção diária, você indica que no momento especificado para a retenção diária, o último ponto de recuperação será mantido para o número de dias especificado. Ou, como outro exemplo, você poderia especificar uma política de retenção mensal para indicar que o ponto de recuperação criado no dia 30 de cada mês deve ser armazenado por 12 meses.

Retenção do ponto de recuperação diários e semanais geralmente coincide com o agendamento de backup. Isso significa que, quando o backup é disparado de acordo com a agenda, o ponto de recuperação criado pelo backup é armazenado pela duração indicada em diária ou semanalmente com a política de retenção.

Por exemplo, na seguinte captura de tela:

- Backups diários em meia-noite e às 18H são mantidos por sete dias.
- Backups feitos em os sábados à meia-noite e às 18H são mantidos por 4 semanas.
- Sábado na última semana do mês em meia-noite e às 18H os backups são mantidos por 12 meses. -Backups feitos em um sábado na última semana de março são mantidos por 10 anos.



Na **Escolher tipo de Backup inicial** especificar como tirar inicial backup, pela rede ou offline. Em seguida, clique em **Próximo**.

Na confirmação, revise as informações e, em seguida, clique em **concluir**.

Depois que o assistente terminar de criar o agendamento de backup, clique em **Fechar**.

3.1.6 EXECUTAR O BACKUP INICIAL OFFLINE

Você pode executar um inicial fazer backup automaticamente pela rede ou offline. A propagação offline de um backup inicial é útil se você tiver grandes quantidades de dados que exigem muita largura de banda de rede para transferir. Você pode fazer uma transferência offline da seguinte maneira:

- Você pode escrever os dados de backup para um local de preparo.
- Você pode usar a ferramenta AzureOfflineBackupDiskPrep para copiar os dados do local de preparo para um ou mais discos SATA.
- A ferramenta cria um trabalho de importação do Azure. Saiba mais sobre exportação e importação do Azure.
- Você pode enviar os discos SATA um datacenter do Azure.
- No datacenter, os dados do disco são copiados para uma conta de armazenamento do Azure.

O Backup do Azure copia os dados da conta de armazenamento para o cofre e backups incrementais são agendados.

3.1.7 HABILITAR A LIMITAÇÃO DE REDE

Você pode controlar como a largura de banda da rede é usada pelo agente de MARS, permitindo a limitação de rede. A limitação é útil se você precisar fazer backup de dados durante o horário de trabalho, mas deseja controlar a largura de banda é usada para o backup e a atividade de restauração.

- Rede de Backup do Azure usa a limitação qualidade de serviço (QoS) no sistema operacional local.

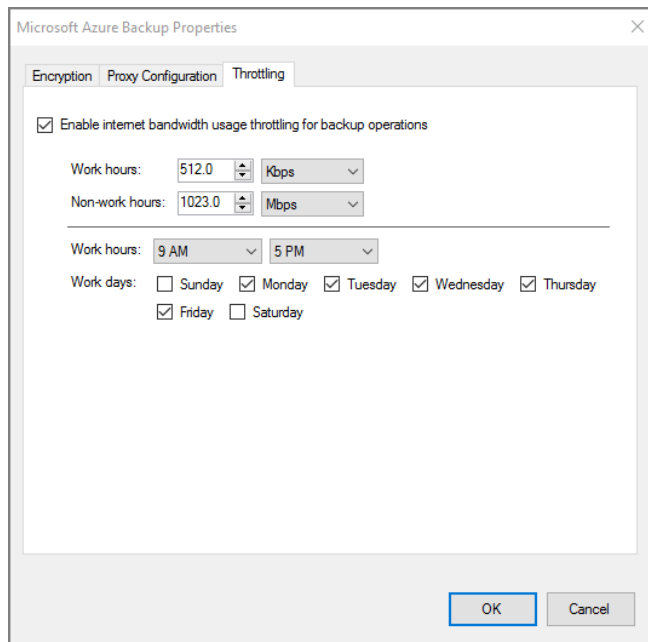
	PROCEDIMENTO	
	ROTINAS DE BACKUP – CLOUD E FITAS	Identificação: PRO-TI-006
		Versão: 01

- Limitação para o backup de rede está disponível no Windows Server 2008 R2 em diante e o Windows 7 em diante. Sistemas operacionais devem estar executando os service packs mais recentes.

Habilite a limitação de rede da seguinte maneira:

No agente de MARS, clique em alterar as propriedades de.

Sobre a limitação guia, seleção habilitar limitação para operações de backup de uso de largura de banda de internet.

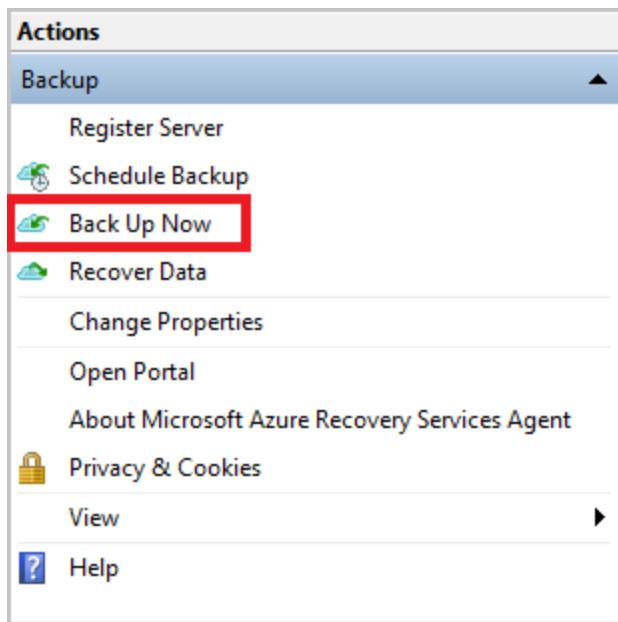


Especifique a largura de banda permitida durante o trabalho e fora do horário de trabalho. Os valores de largura de banda começam em 512 Kbps e ir até 1.023 MBps. Em seguida, clique em **OK**.

3.1.8 Executar um backup ad hoc

No agente de MARS, clique em fazer backup agora. Isso inicia a replicação inicial pela rede.

	PROCEDIMENTO	
	ROTINAS DE BACKUP – CLOUD E FITAS	Identificação: PRO-TI-006
		Versão: 01



Na **confirmação**, examine as configurações e clique em **fazer backup**.

Clique em **Fechar** para fechar o assistente. Se você fizer isso antes do backup for concluído, o assistente continuará a executar em segundo plano.

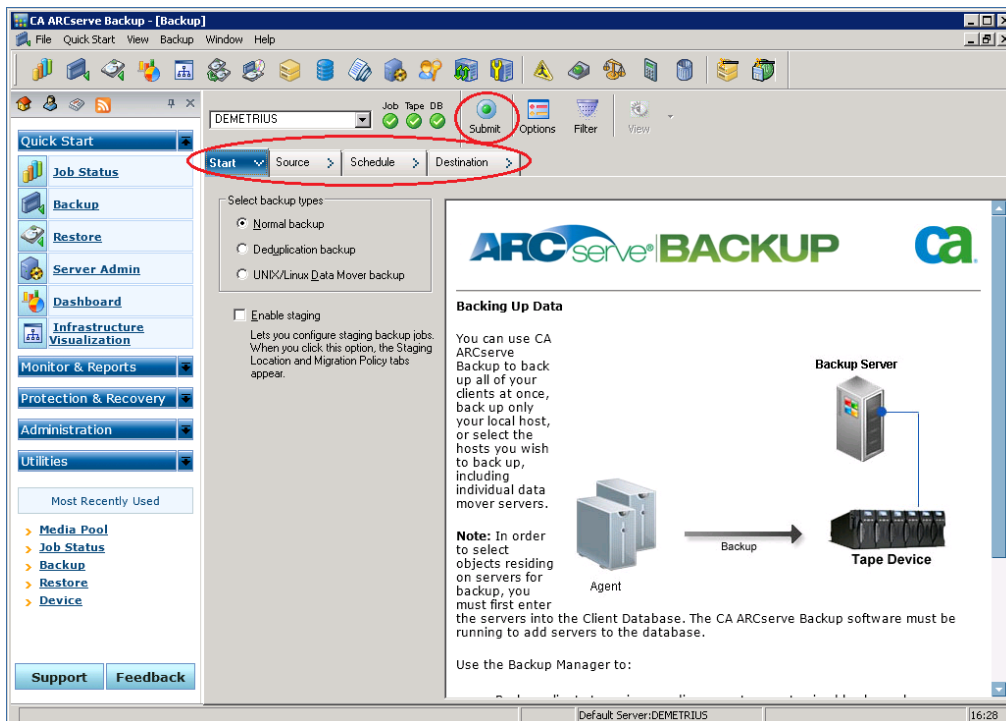
Depois que o backup inicial for concluído, o status **Trabalho concluído** aparecerá no Console de backup.

3.1.9 Criando uma tarefa de backup em Fita.

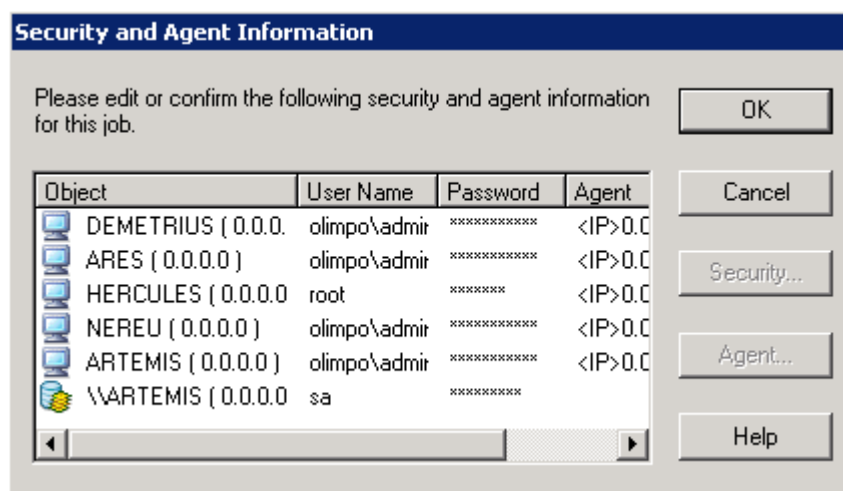
Para criar uma tarefa de backup, abra o aplicativo ARCserve Backup Manager, em seguida clique em “Backup” no menu esquerdo como mostra a figura abaixo:



Uma nova tela será exibida, nela consta as abas necessárias para configuração da tarefa, basta definir a Origem, Agendamento e Destino. Em seguida clique no botão “Submit”.

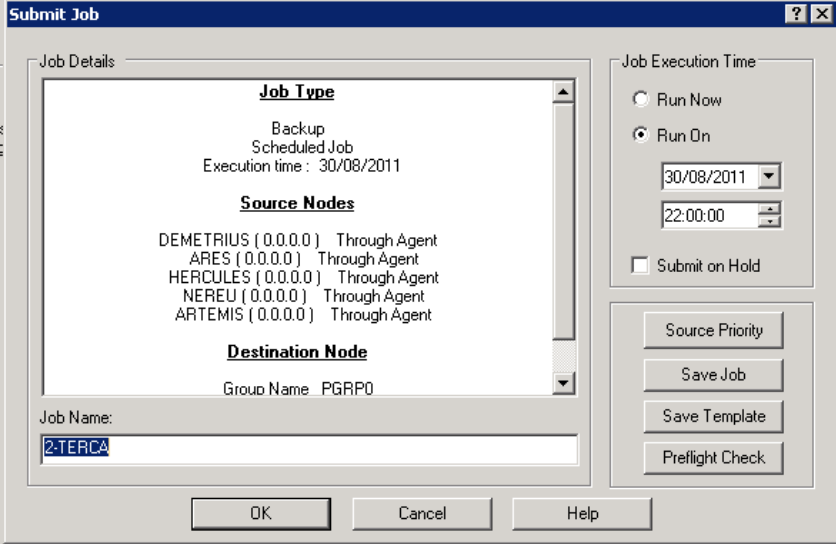


Será exibida uma janela, onde constam as informações de login dos clientes, clique em ok:



Defina um nome para a tarefa, e em que momento a mesma será executada na tela abaixo, em seguida clique no botão “OK” para finalizar.

	PROCEDIMENTO	
	ROTINAS DE BACKUP – CLOUD E FITAS	Identificação: PRO-TI-006
		Versão: 01



4. REFERÊNCIAS

N/A

5. RISCOS

- Falha de sistema
- Sistema inadequado
- Equipamento (Hardware) inadequado
- Impactos nos processos Belliz

6. CONTROLE DE RISCOS

- Backup de informações

7. CONTROLE INTERNOS / KPI's

- N/A

8. CONTROLE E RASTREABILIDADE

Identificação	Responsável	Local	Proteção	Retenção	Disposição
-	-	-	-	-	-

9. CONTROLE DE REVISÕES

Controle de Revisões				
Revisão	Data	Principais Alterações	Elaborado por	Aprovado por
01	12/05/2023	PRIMEIRA PUBLICAÇÃO	Flávio Jefferson Gerente de TI	Flávio Jefferson Gerente de TI

	PROCEDIMENTO	
	ROTINAS DE BACKUP – CLOUD E FITAS	Identificação: PRO-TI-006
		Versão: 01