

# #POWERCON2023

Azure + Veeam:

Proteggere i backup dal ransomware

**Raffaele Valensise**

*Senior Systems Engineer, Veeam Software*  
[raffaele.valensise@veeam.com](mailto:raffaele.valensise@veeam.com)



@rafvalensise



/rvalensise

# Ransomware: la certezza dell'inevitabile

- Il ransomware è una minaccia informatica sempre più diffusa
- Anche adottando solide misure di sicurezza informatica, non è possibile garantire la prevenzione degli attacchi
- Gli aggressori oltre a sfruttare vulnerabilità di servizi e applicazioni, utilizzano tecniche di social engineering avanzate: e-mail di phishing personalizzate, SMS, WhatsApp, LinkedIn o addirittura di persona
- Questi metodi superano le difese digitali dell'organizzazione target



# Obiettivi e impatto degli attacchi ransomware

- Obiettivi degli attacchi sono la crittografia e (sempre più spesso) l'esfiltrazione dei dati dell'organizzazione:
  - È richiesto un pagamento in criptovaluta in cambio della chiave di decrittazione
  - Ulteriore denaro viene richiesto per evitare la divulgazione dei dati sottratti
- Gli attacchi ransomware causano interruzioni nei sistemi informatici, provocando perdite economiche e di reputazione
- La gravità di queste perdite aumenta con il tempo necessario per ripristinare le operazioni



# Proteggere i dati di backup: perché?

- I dati di backup stessi sono uno dei bersagli degli attacchi e possono essere resi inutilizzabili in vari modi:
  - Crittografia
  - Eliminazione / sovrascrittura
  - Contaminazione
- Poiché gli attacchi ransomware si basano spesso sull'acquisizione di credenziali valide all'interno delle rete e successiva escalation di privilegi, **è fondamentale che i dati di backup siano protetti**, anche da possibili attività «pseudo-legittime»



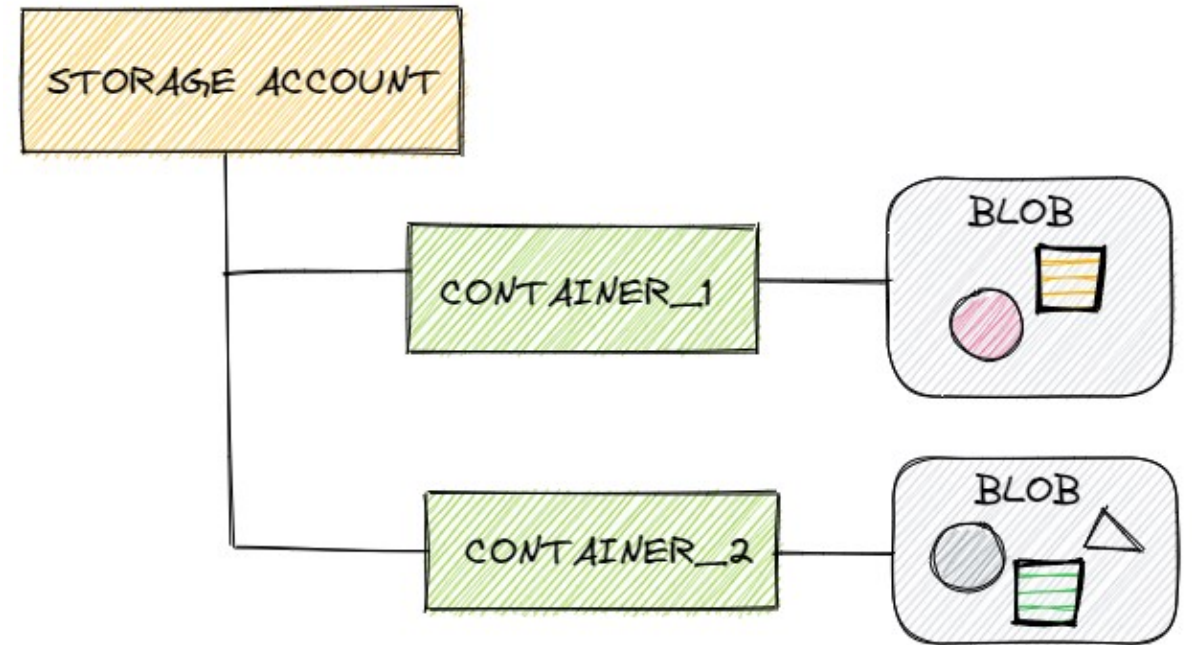
# Proteggere i dati di backup: come?

- Una soluzione fra le più efficaci è di renderli **immutabili**
- Metodologie:
  - Archiviazione su **nastro**
  - Archiviazione su **storage** che offre immutabilità dei dati via file system o con tecnologia proprietaria: NAS, file server, apparati di deduplica, eccetera
  - Archiviazione su **Object Storage**, che offre immutabilità con funzionalità di lock e di versioning – ad esempio, **Azure Blob Storage**



# Azure Blob Storage

- Soluzione Microsoft di **archiviazione ad oggetti** offerta da Azure
- È possibile salvare, modificare, cancellare i dati nei contenitori Blob via HTTP/HTTPS utilizzando API REST, PowerShell e librerie client per .NET, Java, Node.js, Python, PHP, ecc.

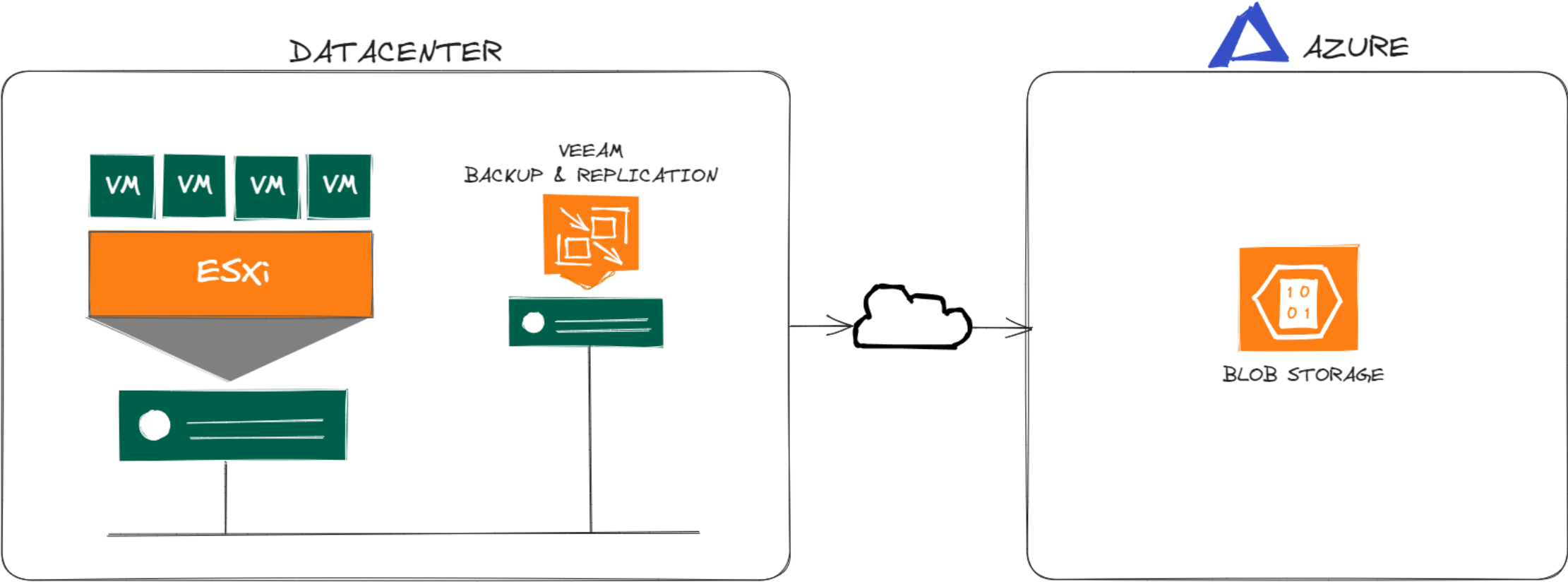


<https://veeamstoragedemo.blob.core.windows.net/backup01>

Storage Account

Container

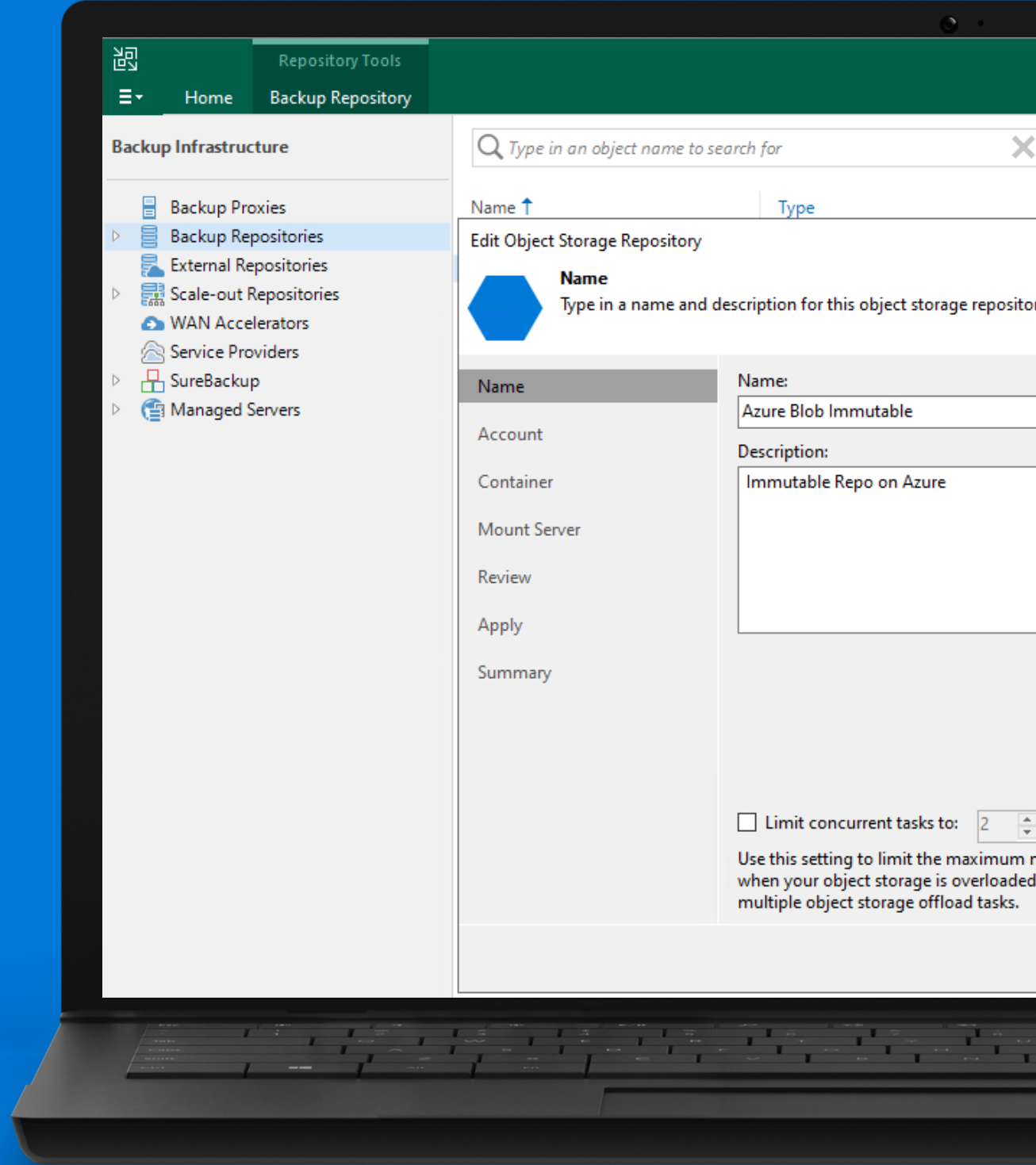
# Scenario Demo





# DEMO

Backup  
immutabili su  
Blob Storage





# Creare uno Storage Account

Home > Create a resource > Marketplace > Storage account >

## Create a storage account

Basics | Advanced | Networking | Data protection | Encryption | Tags | Review

Azure Storage is a Microsoft-managed service providing cloud storage that is highly available, secure, durable, scalable, and redundant. Azure Storage includes Azure Blobs (objects), Azure Data Lake Storage Gen2, Azure Files, Azure Queues, and Azure Tables. The cost of your storage account depends on the usage and the options you choose below. [Learn more about Azure storage accounts](#)

### Project details

Select the subscription in which to create the new storage account. Choose a new or existing resource group to organize and manage your storage account together with other resources.

Subscription \*

Resource group \*   
[Create new](#)

A resource group is a container that holds related resources for an Azure solution.

Name \*

### Instance details

If you need to create a legacy storage account type, please click [here](#).

Storage account name

Region

Performance  Standard: Recommended for most scenarios (general-purpose v2 account)  
 Premium: Recommended for scenarios that require low latency.

Redundancy

Make read access to data available in the event of regional unavailability.

### Instance details

If you need to create a legacy storage account type, please click [here](#).

Storage account name

Region

[Deploy to an edge zone](#)

Performance  Standard: Recommended for most scenarios (general-purpose v2 account)  
 Premium: Recommended for scenarios that require low latency.

Redundancy

Make read access to data available in the event of regional unavailability.

# Creare uno Storage Account

Home > Create a resource > Marketplace > Storage account >

## Create a storage account

Basics **Advanced** Networking Data protection Encryption Tags Review

*Certain options have been disabled by default due to the combination of storage account performance, redundancy, and region.*

### Security

Configure security settings that impact your storage account.

Require secure transfer for REST API operations

Allow enabling public access on containers

Enable storage account key access

Default to Azure Active Directory authorization in the Azure portal

Minimum TLS version

Permitted scope for copy operations (preview)

### Data Lake Storage Gen2

The Data Lake Storage Gen2 hierarchical namespace accelerates big data analytics workloads and enables file-level access control lists (ACLs). [Learn more](#)

Enable hierarchical namespace

[Review](#) [< Previous](#) [Next : Networking >](#)

Home > Create a resource > Marketplace > Storage account >

## Create a storage account

Basics Advanced **Networking** Data protection Encryption Tags Review

### Network connectivity

You can connect to your storage account either publicly, via public IP addresses or service endpoints, or privately, using a private endpoint.

Network access \*

Enable public access from all networks

Enable public access from selected virtual networks and IP addresses

Disable public access and use private access

**i** Enabling public access from all networks might make this resource available publicly. Unless public access is required, we recommend using a more restricted access type. [Learn more](#)

### Network routing

Determine how to route your traffic as it travels from the source to its Azure endpoint. Microsoft network routing is recommended for most customers.

Routing preference  \*

Microsoft network routing

Internet routing

[Review](#) [< Previous](#) [Next : Data protection >](#)

# Creare uno Storage Account

- Disabilitare l'opzione **Enable soft delete for blobs**
- Abilitare l'opzione **Enable versioning for blobs**
- Disabilitare l'opzione **Enable version-level immutability support**.

Home > Create a resource > Marketplace > Storage account >

## Create a storage account

Basics Advanced Networking Data protection Encryption Tags Review

### Recovery

Protect your data from accidental or erroneous deletion or modification.

Enable point-in-time restore for containers  
Use point-in-time restore to restore one or more containers to an earlier state. If point-in-time restore is enabled, then versioning, change feed, and blob soft delete must also be enabled. [Learn more](#)

**Enable soft delete for blobs**  
Soft delete enables you to recover blobs that were previously marked for deletion, including blobs that were overwritten. [Learn more](#)

Days to retain deleted blobs

Enable soft delete for containers  
Soft delete enables you to recover containers that were previously marked for deletion. [Learn more](#)

Days to retain deleted containers

Enable soft delete for file shares  
Soft delete enables you to recover file shares that were previously marked for deletion. [Learn more](#)

Days to retain deleted file shares

### Tracking

Manage versions and keep track of changes made to your blob data.

**Enable versioning for blobs**  
Use versioning to automatically maintain previous versions of your blobs. [Learn more](#)

Consider your workloads, their impact on the number of versions created, and the resulting costs. Optimize costs by automatically managing the data lifecycle. [Learn more](#)

Enable blob change feed  
Keep track of create, modification, and delete changes to blobs in your account. [Learn more](#)

### Access control

**Enable version-level immutability support**  
Allows you to set time-based retention policy on the account-level that will apply to all blob versions. Enable this feature to set a default policy at the account level. Without enabling this, you can still set a default policy at the container level or set policies for specific blob versions. Versioning is required for this property to be enabled. [Learn more](#)

# Creare un Container

veeamstoragedemo  
Storage account

Search

Upload Open in Explorer

Essentials

Resource group (move) : veeamdemo

Location : West Europe

Primary/Secondary Location : Primary: Wes

Subscription (move) : Enterprise

Subscription ID : 2550c090-2c

Disk state : Primary: Avail

Tags (edit) : Click here to

Overview

Activity log

Tags

Diagnose and solve problems

Access Control (IAM)

Data migration

Events

Storage browser

Data storage

**Containers**

File shares

Selezionare l'opzione **Enable version-level immutability support**

veeamstoragedemo | Containers  
Storage account

Search

**+ Container** Change access level Restore containers Refresh

Search containers by prefix

Name

\$logs

New container

Name \*

backup01

Public access level ⓘ

Private (no anonymous access)

Advanced

Encryption scope

Select from existing account scopes

Use this encryption scope for all blobs in the container

Enable version-level immutability support ⓘ

# Creare un Container

veeamstoragedemo | Containers

Storage account

Search

+ Container Change access level restore containers

Search containers by prefix

Name

- \$logs
- backup01

Overview

Activity log

Tags

Diagnose and solve problems

Access Control (IAM)

Data migration

Events

Storage browser

Data storage

Containers

File shares

Queues

Tables

Security + networking

Networking

Azure CDN

Access keys

veeamstoragedemo | Access keys

Storage account

Search

Set rotation reminder Refresh Give feedback

Access keys authenticate your applications' requests to this storage account. Keep your keys in a secure location like Azure Key Vault, and replace them often with new keys. The two keys allow you to replace one while still using the other.

Remember to update the keys with any Azure resources and apps that use this storage account. [Learn more about managing storage account access keys](#)

Storage account name

veeamstoragedemo

key1 Rotate key

Last rotated: 14/3/2023 (0 days ago)

Key

..... Show

Connection string

..... Show

# Aggiungere il Container a Veeam Backup & Replication

The screenshot displays the Veeam Backup & Replication console. The left sidebar shows the 'Backup Infrastructure' section, with 'Backup Repositories' highlighted. A red box highlights the 'Add backup repository...' button. The main area shows a table with columns for Name, Type, Host, and Path. A search bar is visible above the table.

The 'Add Backup Repository' dialog box is open, showing the following options:

- Direct attached storage**: Microsoft Windows or Linux server with internal or direct attached storage. This configuration enables data movers to run directly on the server, allowing for fastest performance.
- Network attached storage**: Network share on a file server or a NAS device. When backing up to a remote share, we recommend that you select a gateway server located in the same site with the share.
- Deduplicating storage appliance**: Dell Data Domain, ExaGrid, Fujitsu ETERNUS CS800, HPE StoreOnce, Infinidat InfiniGuard or Quantum D are unable to meet the requirements of advanced integration via native appliance API, use the network storage option instead.
- Object storage**: On-prem object storage system or a cloud object storage provider.

The 'Object Storage' dialog box is also open, showing the following options:

- S3 Compatible**: Adds an on-premises object storage system or a cloud object storage provider.
- Amazon S3**: Adds Amazon cloud object storage. Amazon S3, Amazon S3 Glacier (including Deep Archive) and Amazon Snowball Edge are supported.
- Google Cloud Storage**: Adds Google Cloud storage. Both Standard and Nearline storage classes are supported.
- IBM Cloud Object Storage**: Adds IBM Cloud object storage. S3 compatible versions of both on-premises and IBM Cloud storage offerings are supported.
- Microsoft Azure Storage**: Adds Microsoft Azure cloud object storage. Microsoft Azure Blob Storage, Microsoft Azure Archive Storage and Microsoft Azure Data Box are supported.
- Wasabi Cloud Storage**: Adds Wasabi cloud object storage.

A 'Cancel' button is visible at the bottom right of the 'Object Storage' dialog.

# Aggiungere il Container a Veeam Backup & Replication

The image displays a sequence of four overlapping windows from the Veeam Backup & Replication software, illustrating the steps to add a new Object Storage Repository for Microsoft Azure Storage.

- Microsoft Azure Storage:** The initial window where the user selects the type of Azure storage to use as a backup repository. The "Azure Blob Storage" option is highlighted.
- New Object Storage Repository (Step 1):** The user enters the repository name "Immutable Blob" and the description "Azure Blob Storage + Immutability".
- New Object Storage Repository (Step 2):** The user specifies the account to use for connecting to Microsoft Azure blob storage. The "Add..." button is highlighted.
- Credentials:** The user enters the account name "veeamstoragedemo" and the shared key (masked with dots). The "OK" button is highlighted.



# Aggiungere il Container a Veeam Backup & Replication

New Object Storage Repository

**Container**  
Specify Microsoft Azure blob storage container to use.

Name: Container  
Account: backup01  
Container: Folder: Browse...

Mount Server  
Review  
Apply  
Summary

Limit object storage consumption to: 10 TB  
This is a soft limit to help control your object storage spend. If the specified limit is exceeded, already running backup offload tasks will be allowed to complete, but no new tasks will be started.

Make recent backups immutable for: 30 days  
Protects backups from modification or deletion by ransomware, malicious insiders and hackers. GFS backups are made immutable for the entire duration of their retention policy.

Use cool blob storage tier (may result in higher costs)  
With lower price per GB but higher retrieval and early deletion fees, this storage tier is best suited for storing long-term backups such as GFS fulls.

< Previous Next > Finish

Select Folder

Folders:

- backup01
- VMs

New Folder OK Cancel

New Object Storage Repository

**Container**  
Specify Microsoft Azure blob storage container to use.

Name: Container  
Account: backup01  
Container: Folder: VMs Browse...

Mount Server  
Review  
Apply  
Summary

Limit object storage consumption to: 10 TB  
This is a soft limit to help control your object storage spend. If the specified limit is exceeded, already running backup offload tasks will be allowed to complete, but no new tasks will be started.

Make recent backups immutable for: 30 days  
Protects backups from modification or deletion by ransomware, malicious insiders and hackers. GFS backups are made immutable for the entire duration of their retention policy.

Use cool blob storage tier (may result in higher costs)  
With lower price per GB but higher retrieval and early deletion fees, this storage tier is best suited for storing long-term backups such as GFS fulls.

< Previous Next > Finish Cancel

# Configurare un job di backup

The image shows the Veeam Backup and Replication interface. The main window displays the 'Home' tab with various job types. The 'Backup Job' menu is open, and 'Virtual machine' is selected. Under 'Virtual machine', 'VMware vSphere...' is highlighted. The 'New Backup Job' dialog box is open, showing the 'Storage' configuration page. The 'Storage' page includes the following settings:

- Name:** Virtual Machines
- Backup proxy:** Automatic selection
- Backup repository:** Immutable Blob (Azure Blob Storage + Immutability)
- Guest Processing:** N/A
- Retention policy:** 60 days
- Keep certain full backups longer for archival purposes
- Configure secondary destinations for this job

The 'Next >' button at the bottom of the dialog is highlighted with a red box, indicating the next step in the configuration process.

# Verificare l'efficacia dell'immutabilità

The screenshot shows the Veeam Backup and Replication console. A search bar at the top contains the text "Type in an object name to search for". Below it, a table lists backup jobs. The "VM Backup" job is selected, and a context menu is open over it. The menu items are: "Move backup...", "Copy backup...", "Detach from job", "Delete from disk" (highlighted with a red box), and "Properties...".

Job Name ↑	Creation Time	Restore Points	Platform
VM Backup	3/15/2023 12:52 PM	1	VMware

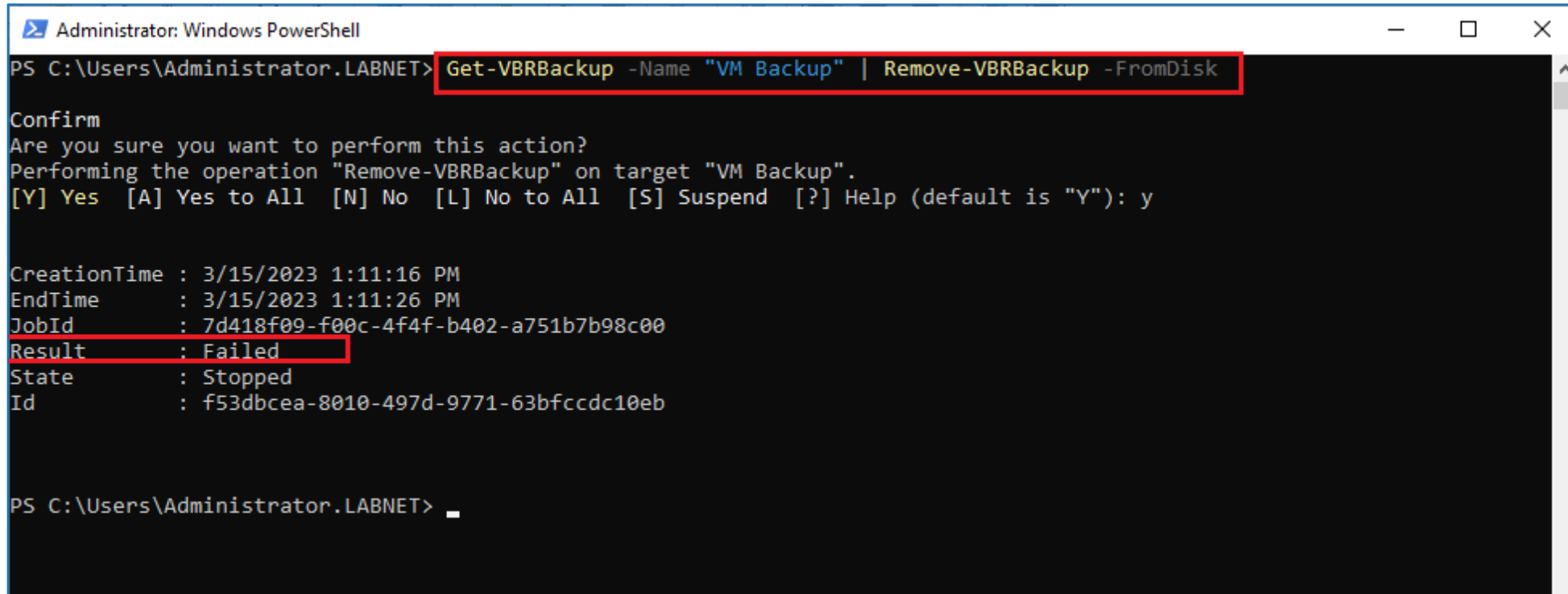
A confirmation dialog box titled "Veeam Backup and Replication" with a question mark icon. The text reads "Delete backups from object storage?". There are two buttons: "Yes" (highlighted with a red box) and "No".

The screenshot shows the "Removing backup" job log. The job name is "Backup Deletion Job" and its status is "Failed". The action type is "Backup Deletion", initiated by "LABNET\Administrator". The start time is "3/15/2023 1:05:59 PM" and the end time is "3/15/2023 1:06:09 PM".

Message	Duration
Starting backup deletion job	
Preparing objects for deletion	
Building tasks list	
Processing backup 1 out of 1 (100% done)	0:00:08
[VM Backup - SRV-INTERACT-01] Failed to delete backup Error: Unable to delete t...	0:00:06
Immutable Blob: 0 deleted, 0 skipped, 0 warned, 1 failed	
Job finished with error at 3/15/2023 1:06:09 PM	

# Verificare l'efficacia dell'immutabilità

```
Get-VBRBackup -Name "VM Backup" | Remove-VBRBackup -FromDisk
```



The screenshot shows a Windows PowerShell terminal window titled "Administrator: Windows PowerShell". The command `Get-VBRBackup -Name "VM Backup" | Remove-VBRBackup -FromDisk` is entered and highlighted with a red box. The terminal displays a confirmation prompt: "Confirm Are you sure you want to perform this action? Performing the operation 'Remove-VBRBackup' on target 'VM Backup'. [Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is 'Y'): y". The output shows the following properties: `CreationTime : 3/15/2023 1:11:16 PM`, `EndTime : 3/15/2023 1:11:26 PM`, `JobId : 7d418f09-f00c-4f4f-b402-a751b7b98c00`, `Result : Failed` (highlighted with a red box), `State : Stopped`, and `Id : f53dbcea-8010-497d-9771-63bfccdc10eb`. The terminal ends with the prompt `PS C:\Users\Administrator.LABNET>`.

```
Administrator: Windows PowerShell
PS C:\Users\Administrator.LABNET> Get-VBRBackup -Name "VM Backup" | Remove-VBRBackup -FromDisk
Confirm
Are you sure you want to perform this action?
Performing the operation "Remove-VBRBackup" on target "VM Backup".
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "Y"): y

CreationTime : 3/15/2023 1:11:16 PM
EndTime       : 3/15/2023 1:11:26 PM
JobId        : 7d418f09-f00c-4f4f-b402-a751b7b98c00
Result       : Failed
State        : Stopped
Id           : f53dbcea-8010-497d-9771-63bfccdc10eb

PS C:\Users\Administrator.LABNET>
```

# Grazie

Raffaele Valensise

*Senior Systems Engineer, Veeam Software*  
*raffaele.valensise@veeam.com*



@rafvalensise



/rvalensise