ICT POWER.IT

Microsoft

#POWERCON2023

Azure + Veeam:
Proteggere i backup dal ransomware

Raffaele Valensise
Senior Systems Engineer, Veeam Software
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'esflitrazione 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

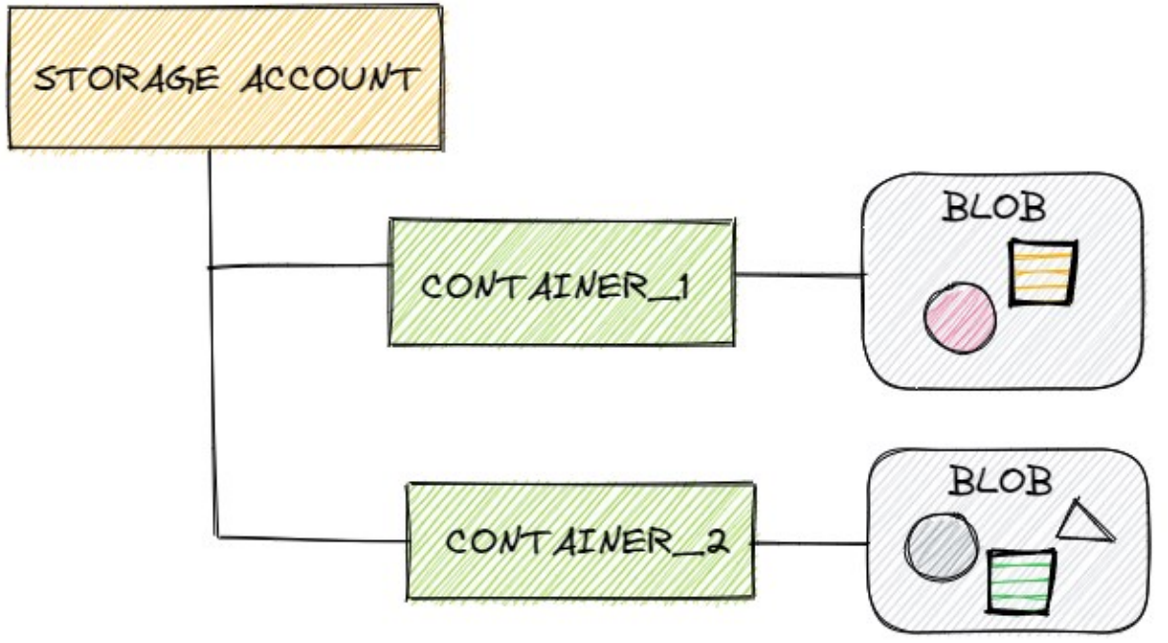
- Poiché gli attacchi ransomware si basano spesso sull'acquisizione di credenziali valide all'interno delle rete e successiva escalation di privilegi, **è fondamentale che i dati di backup siano protetti**, anche da possibili attività «pseudo-legittime»

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.

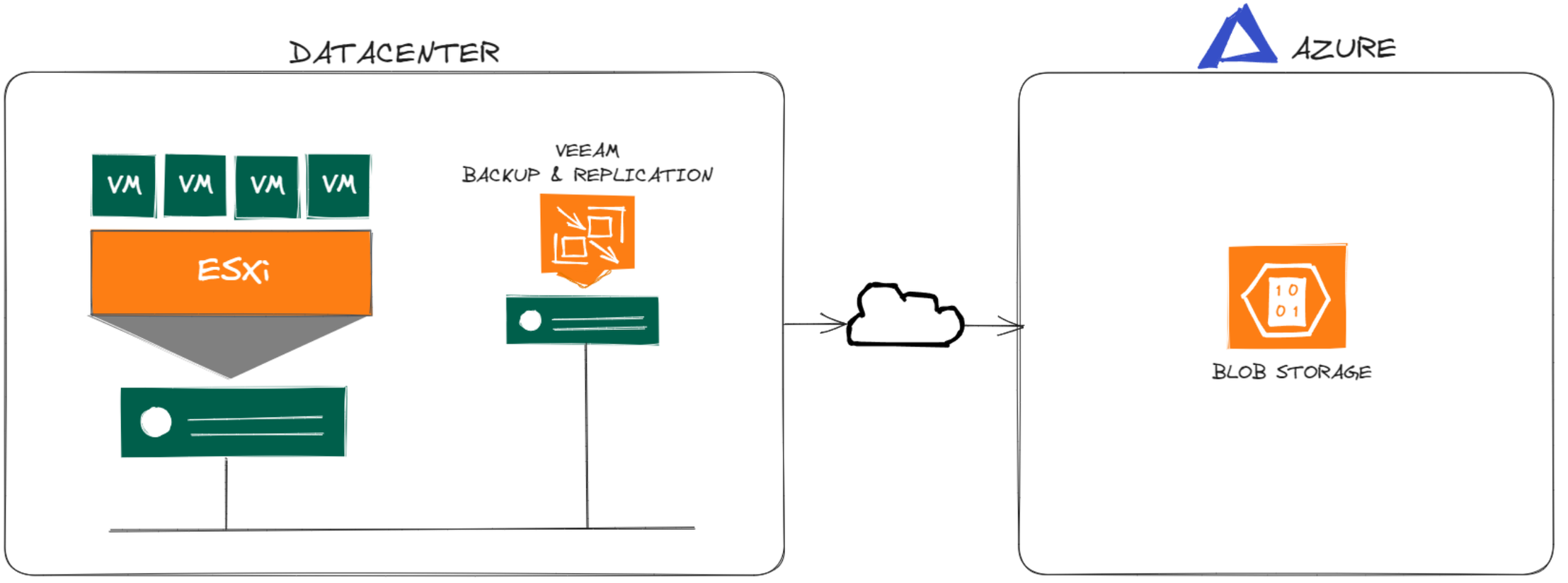


https://veeamstoragedemo.blob.core.windows.net/backup01

Storage Account

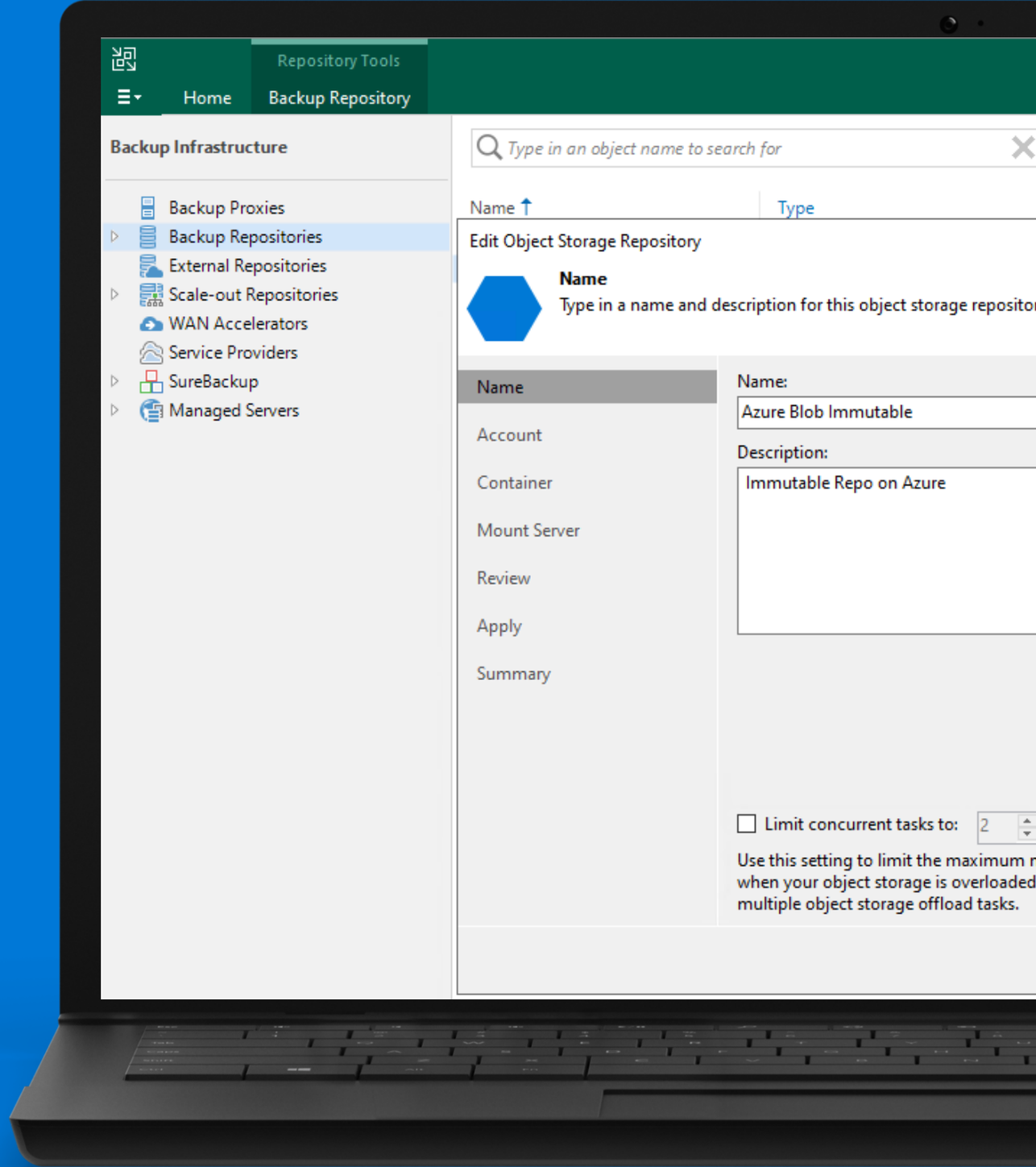
Container

Scenario Demo

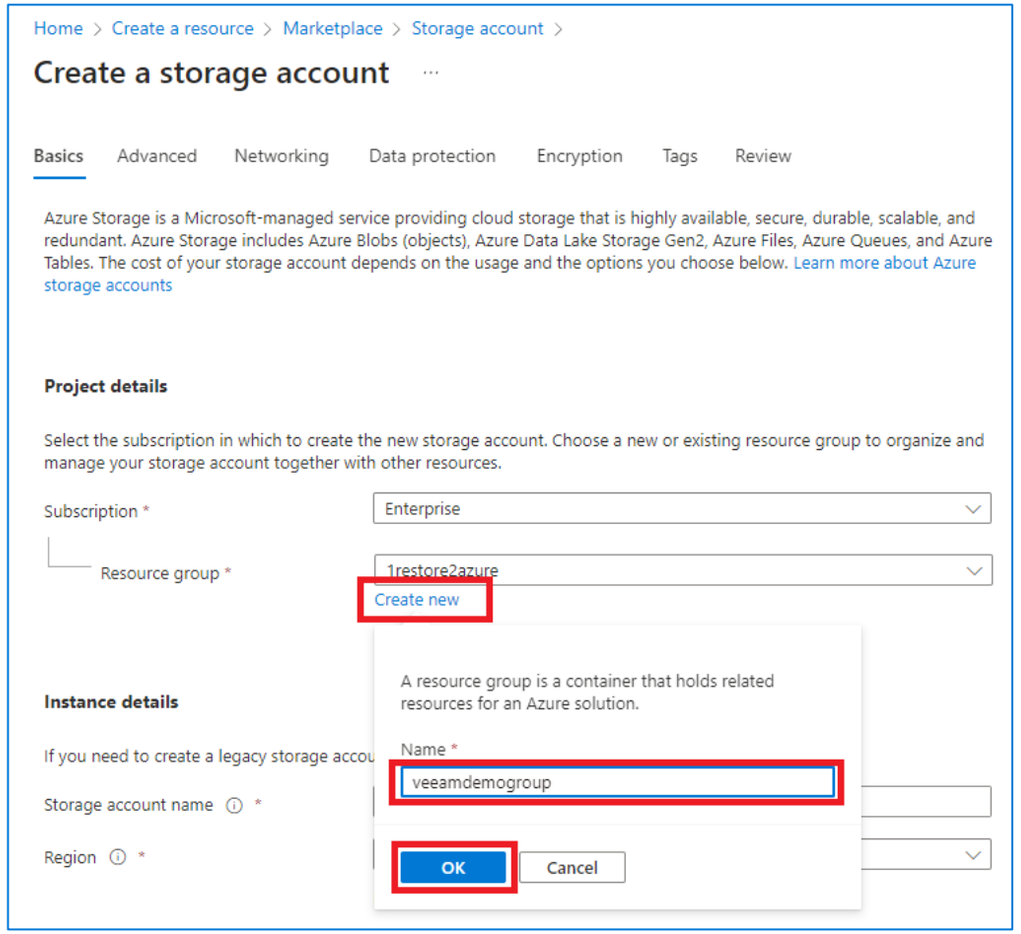


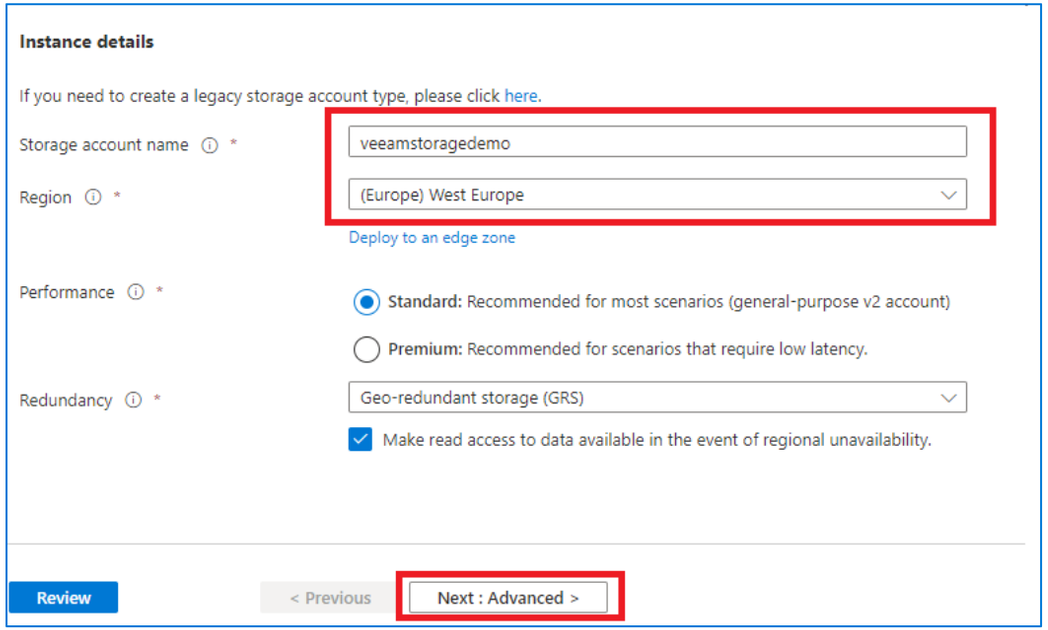
DEMO

Backup immutabili su Blob Storage

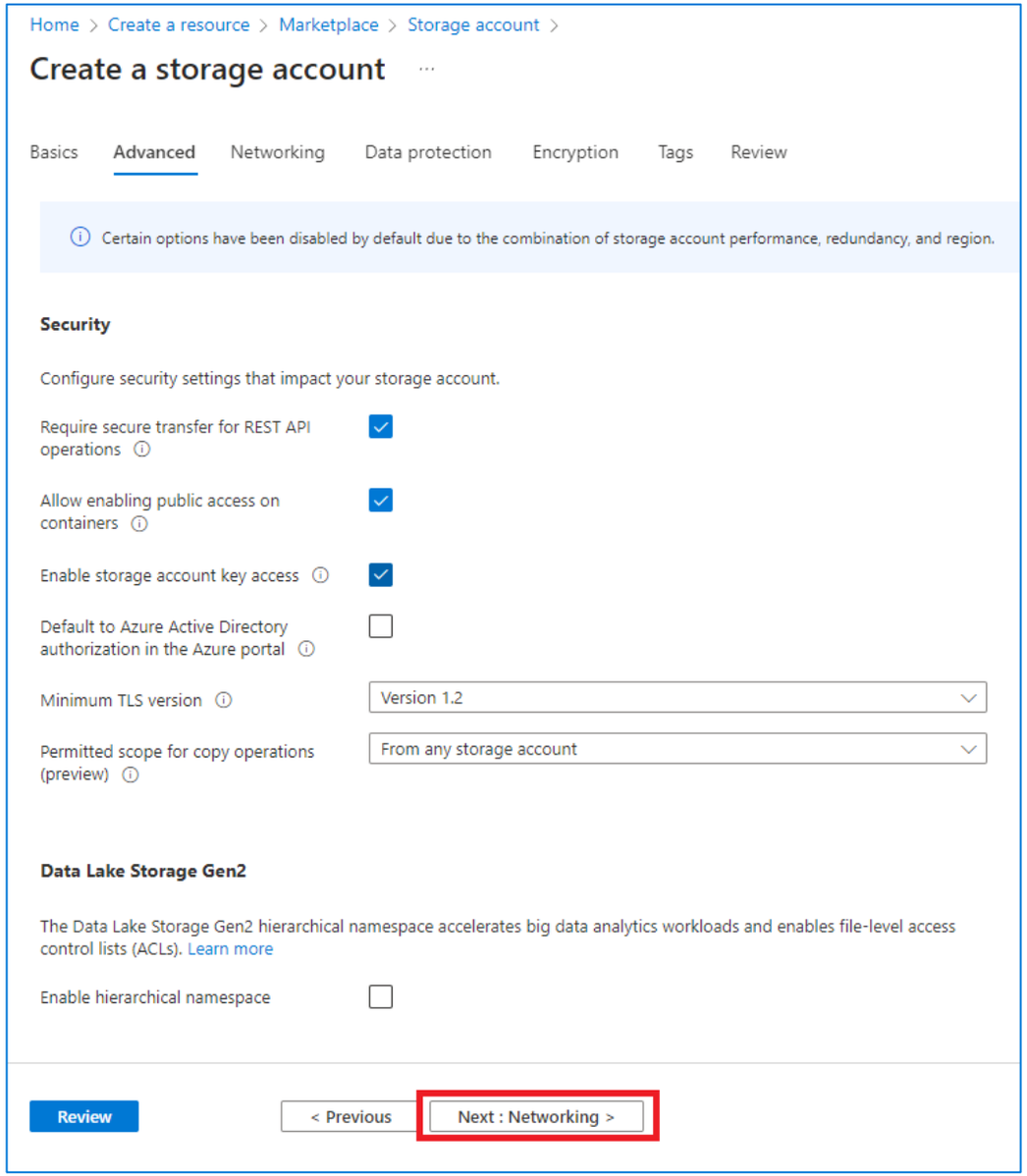


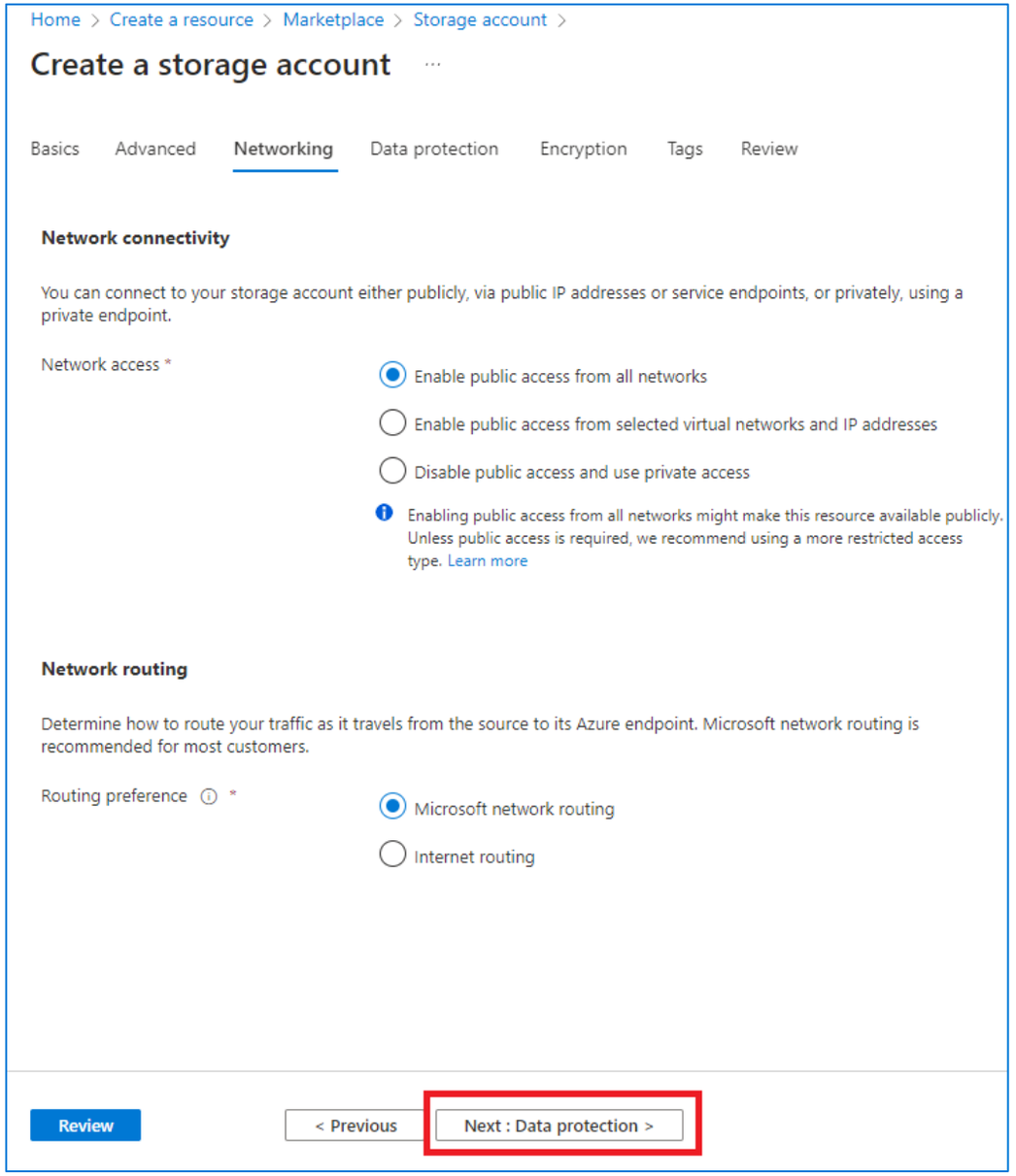
Creare uno Storage Account





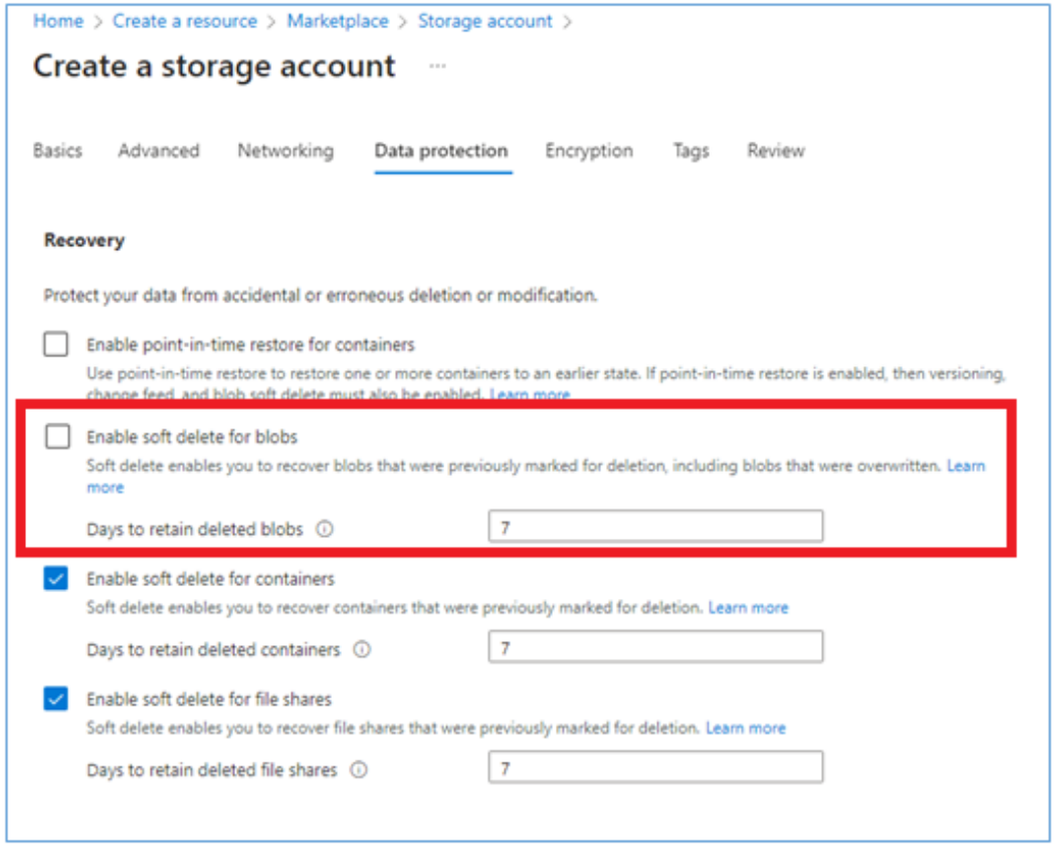
Creare uno Storage Account

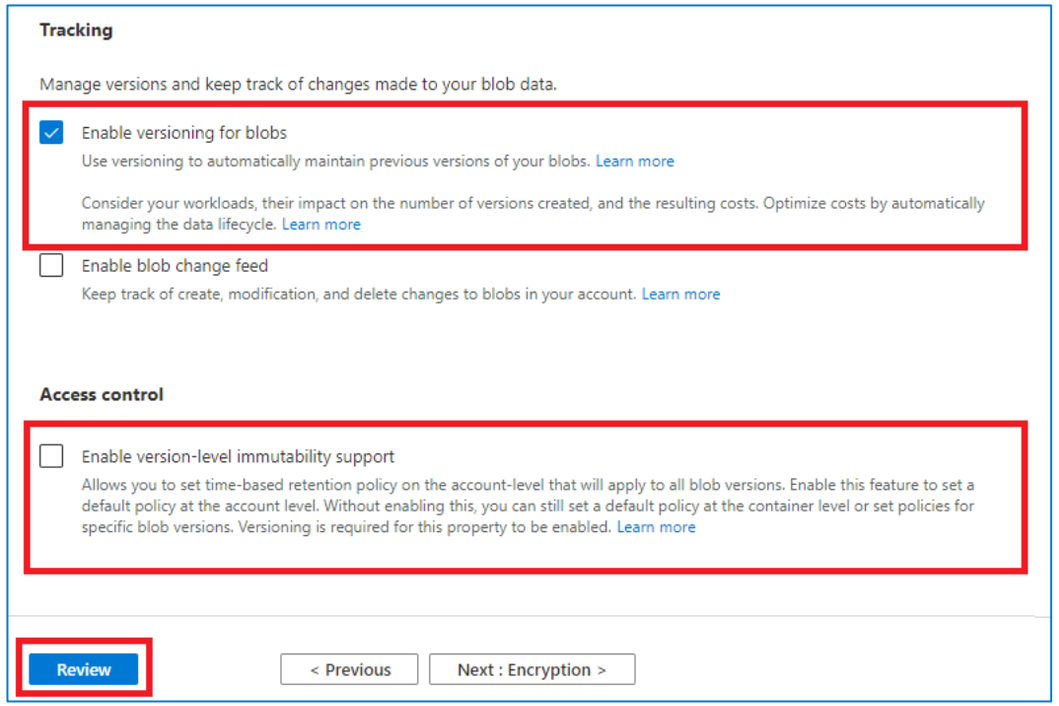




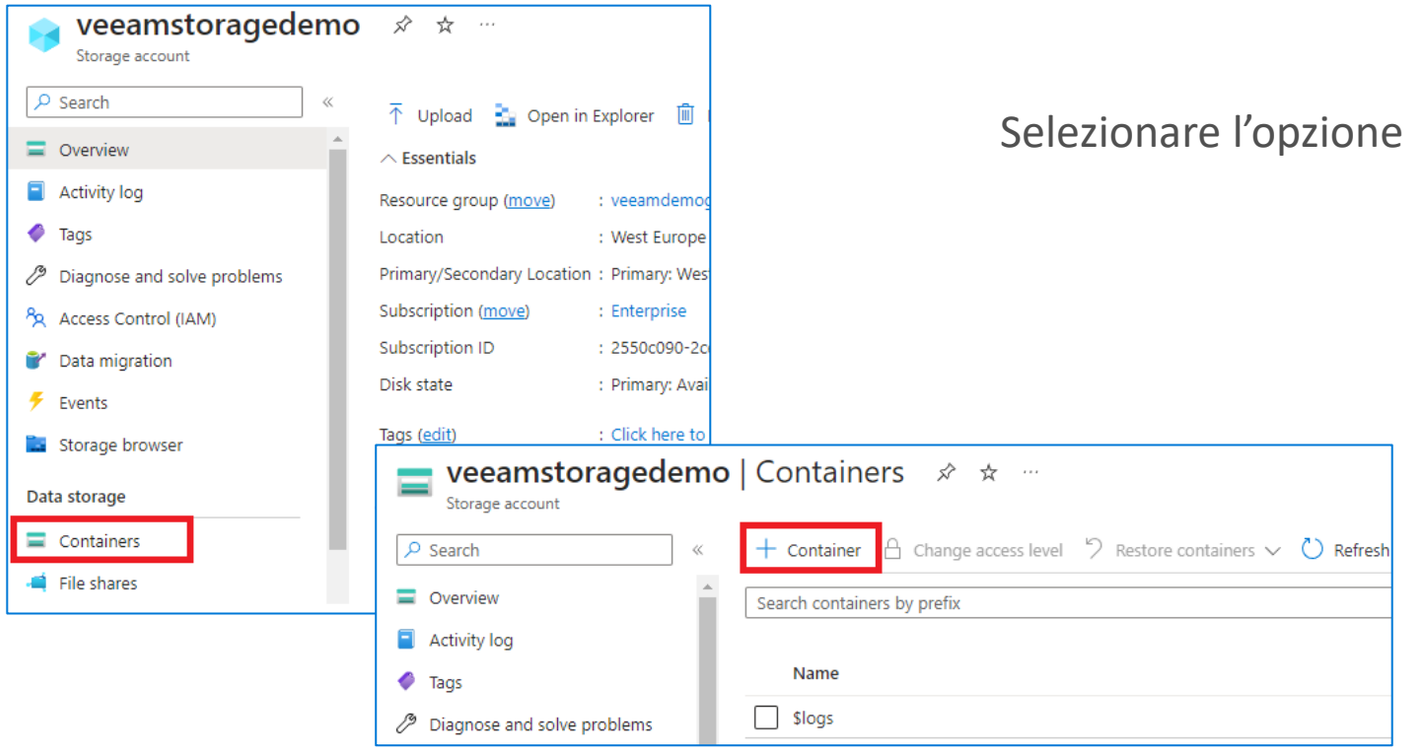
Creare uno Storage Account

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

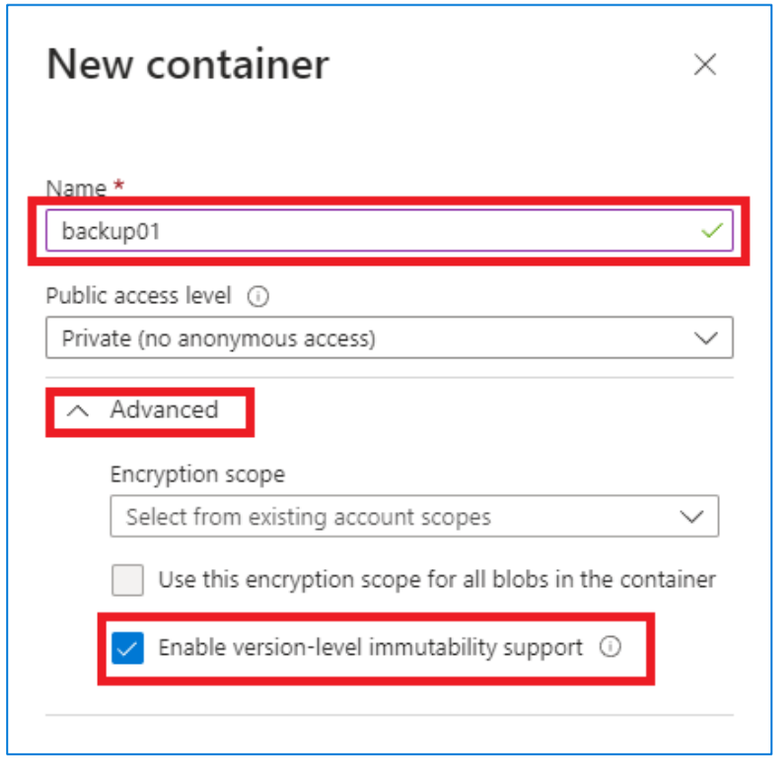




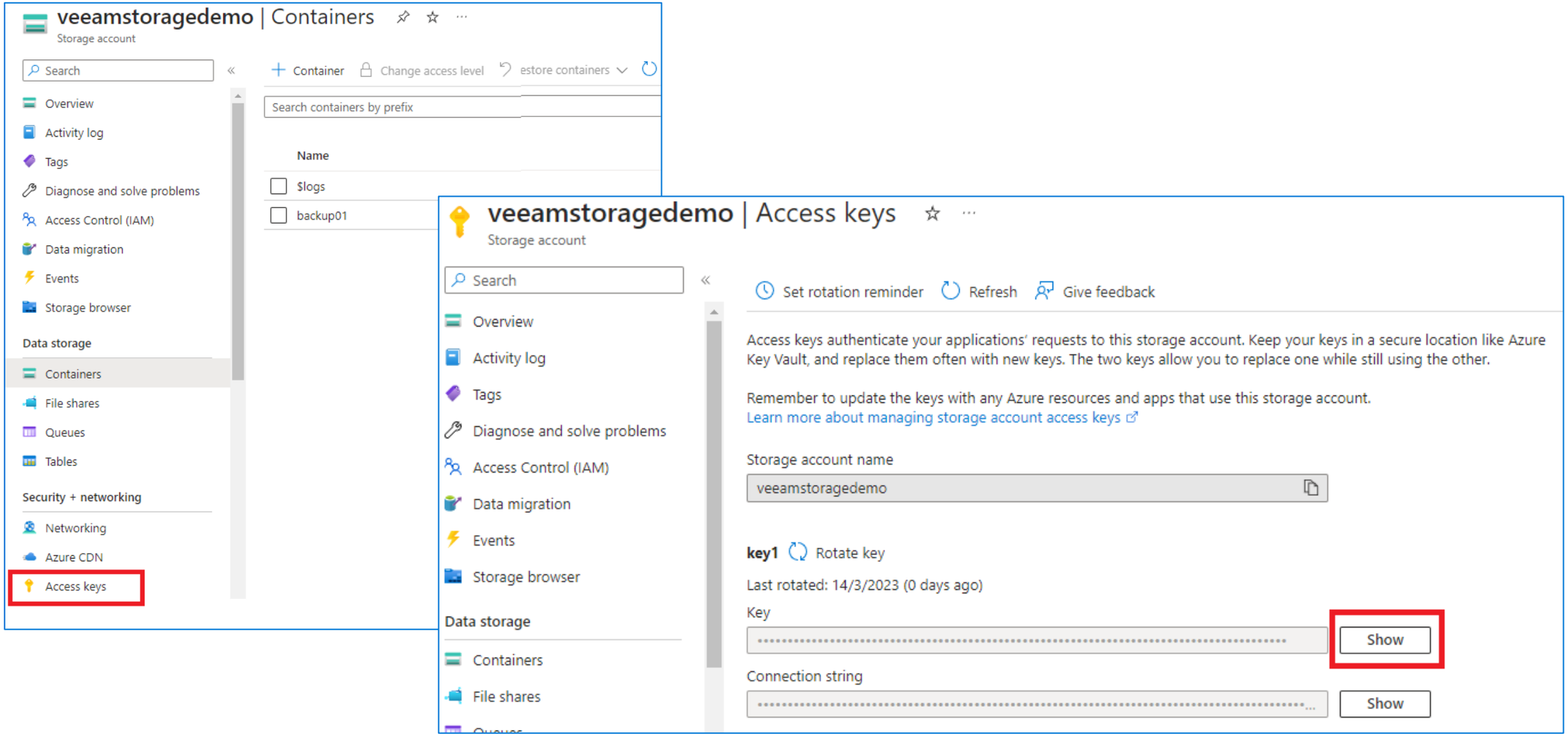
Creare un Container



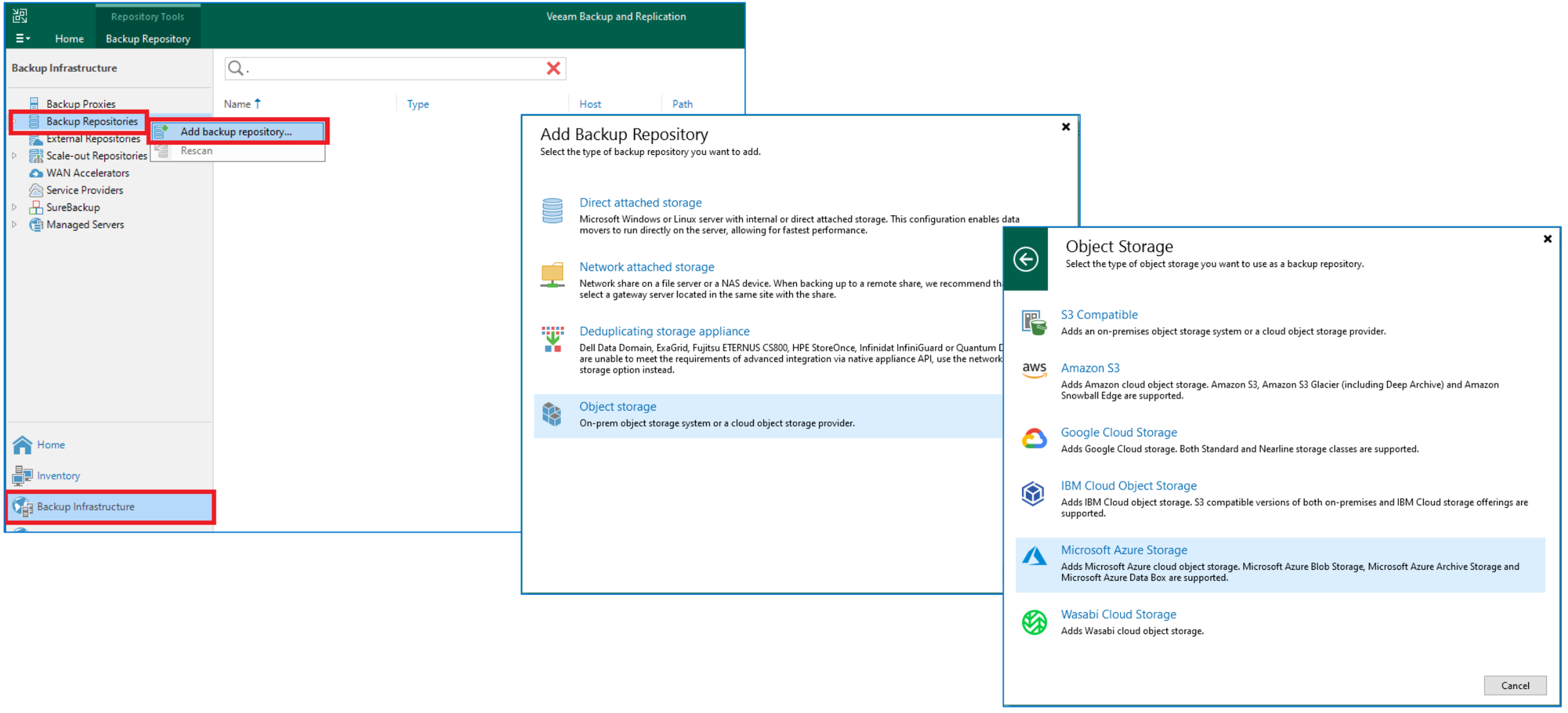
Selezionare l'opzione **Enable version-level immutability support**



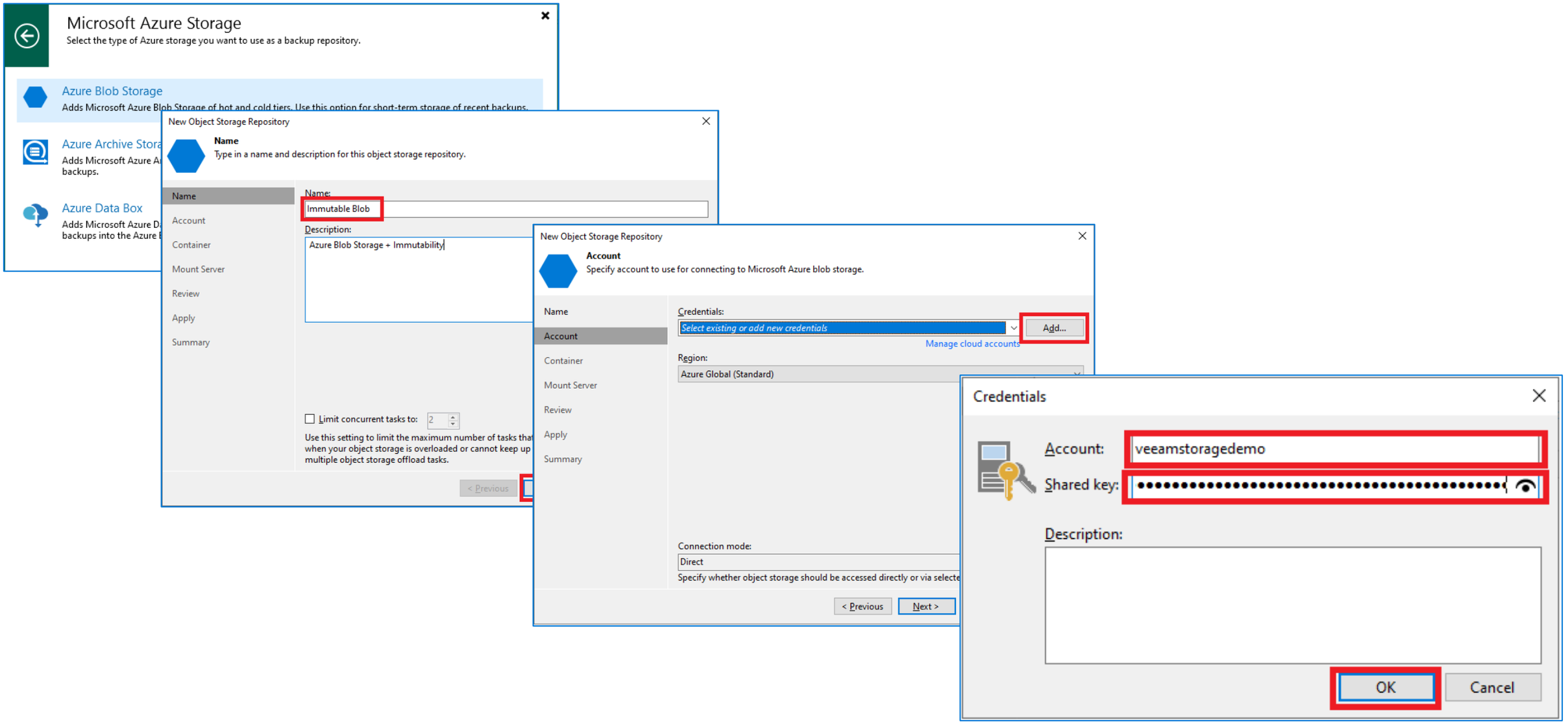
Creare un Container



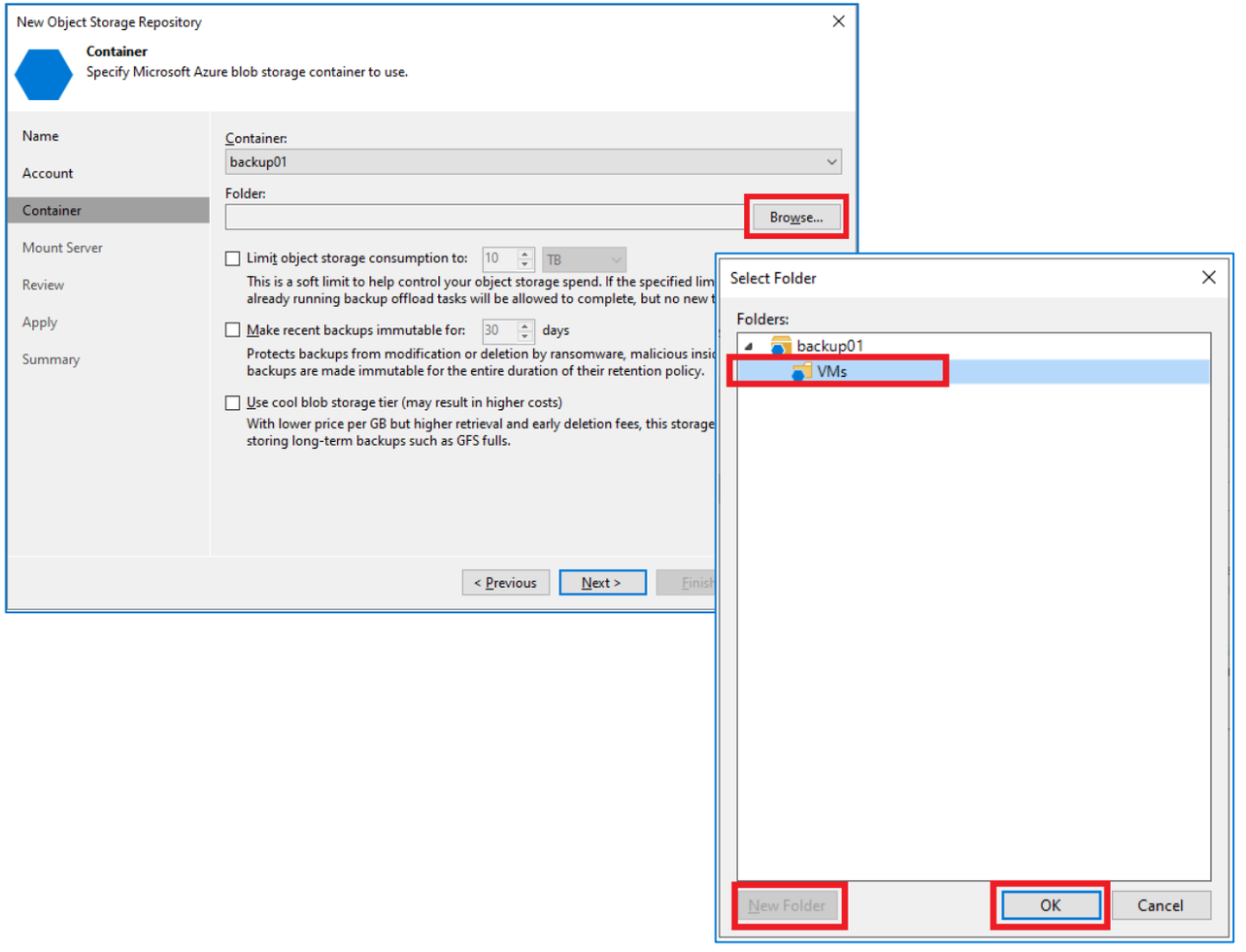
Aggiungere il Container a Veeam Backup & Replication

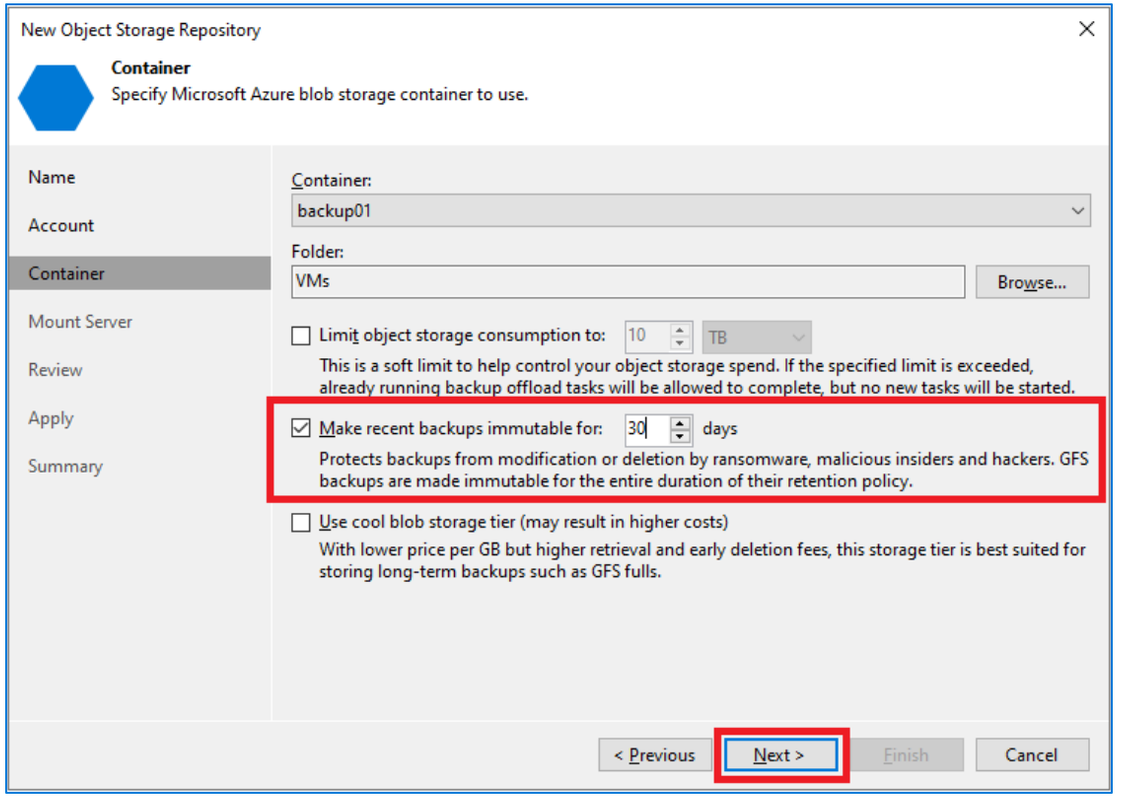


Aggiungere il Container a Veeam Backup & Replication

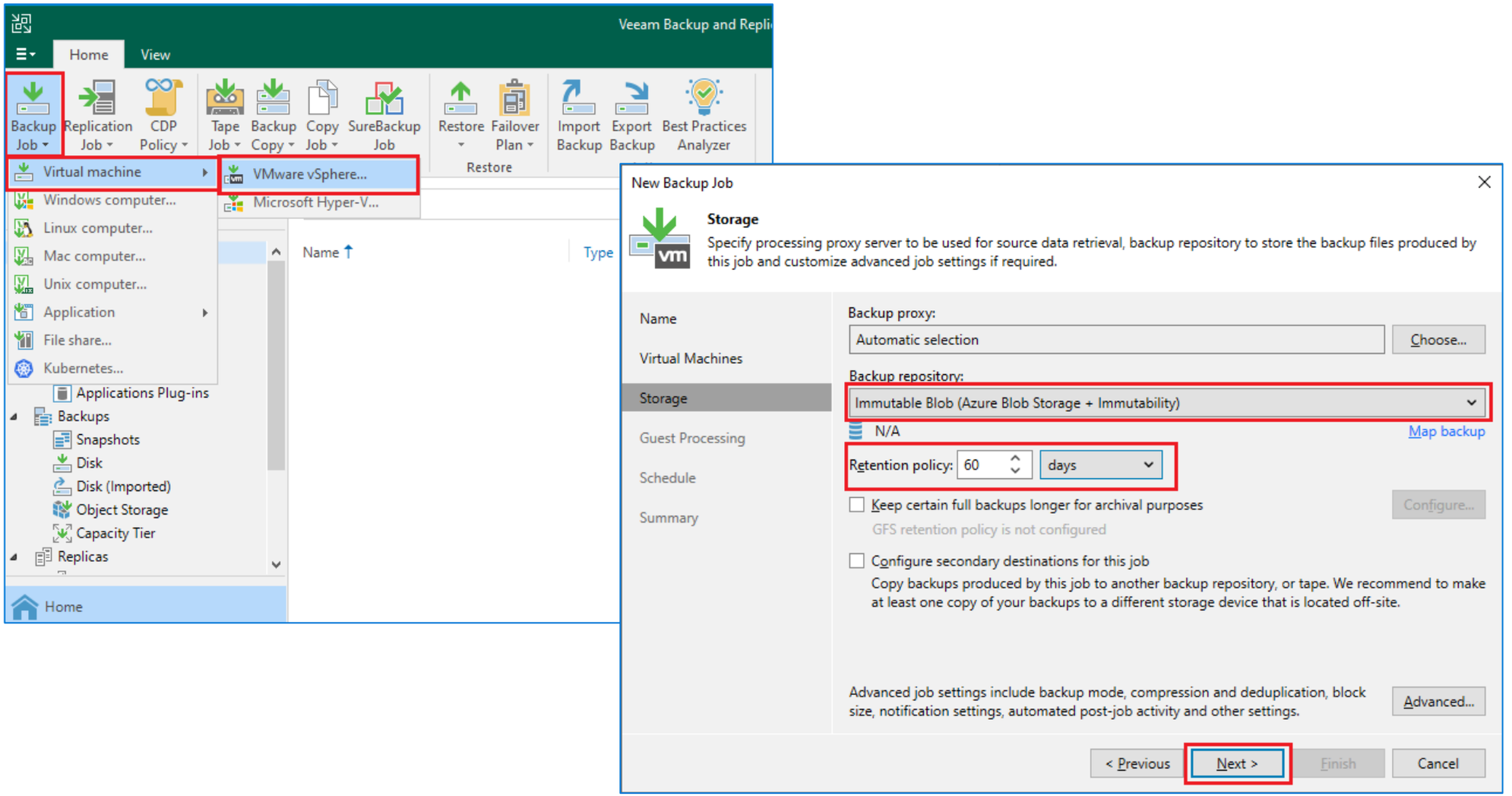


Aggiungere il Container a Veeam Backup & Replication

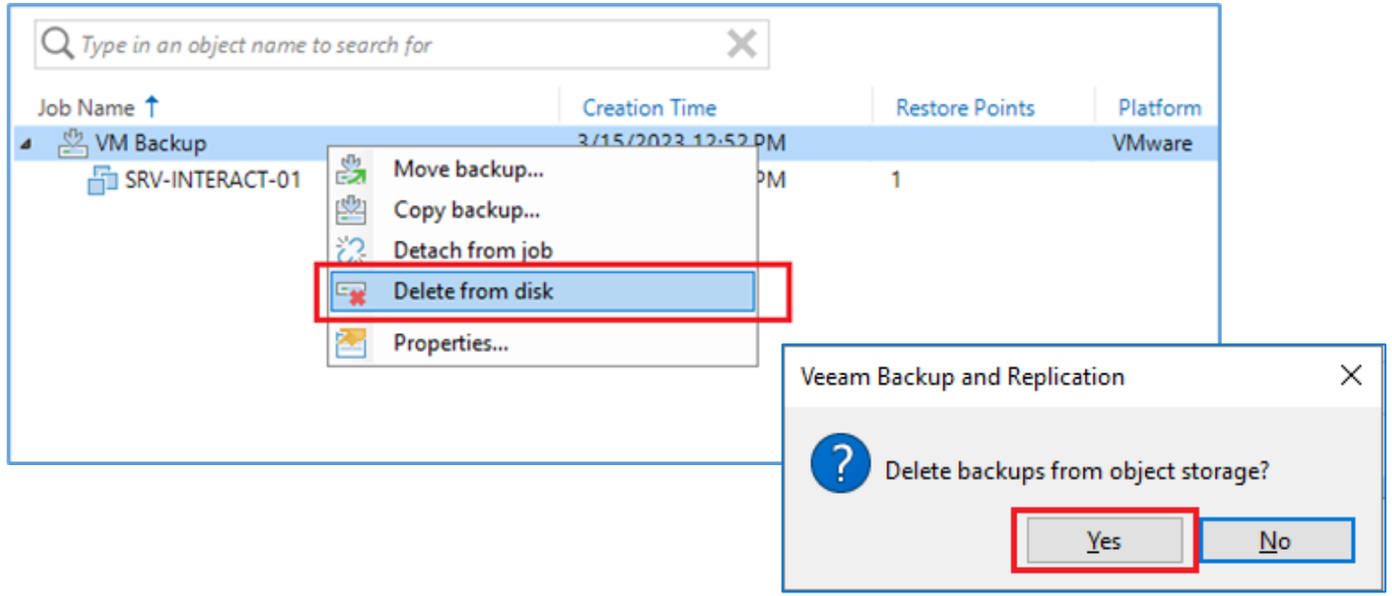


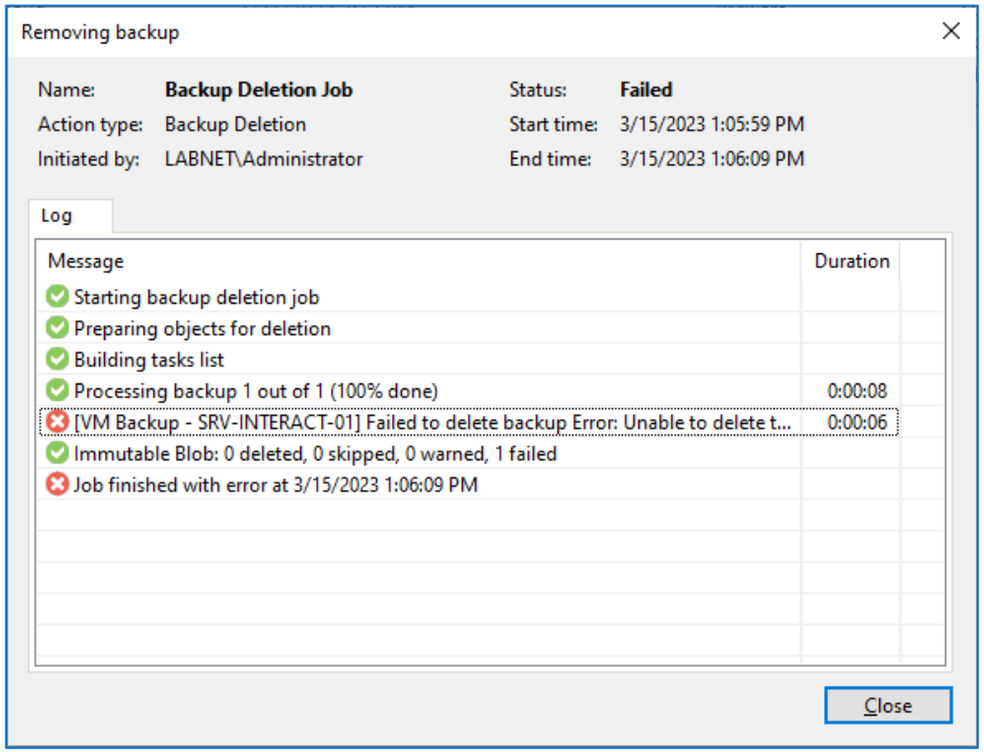


Configurare un job di backup



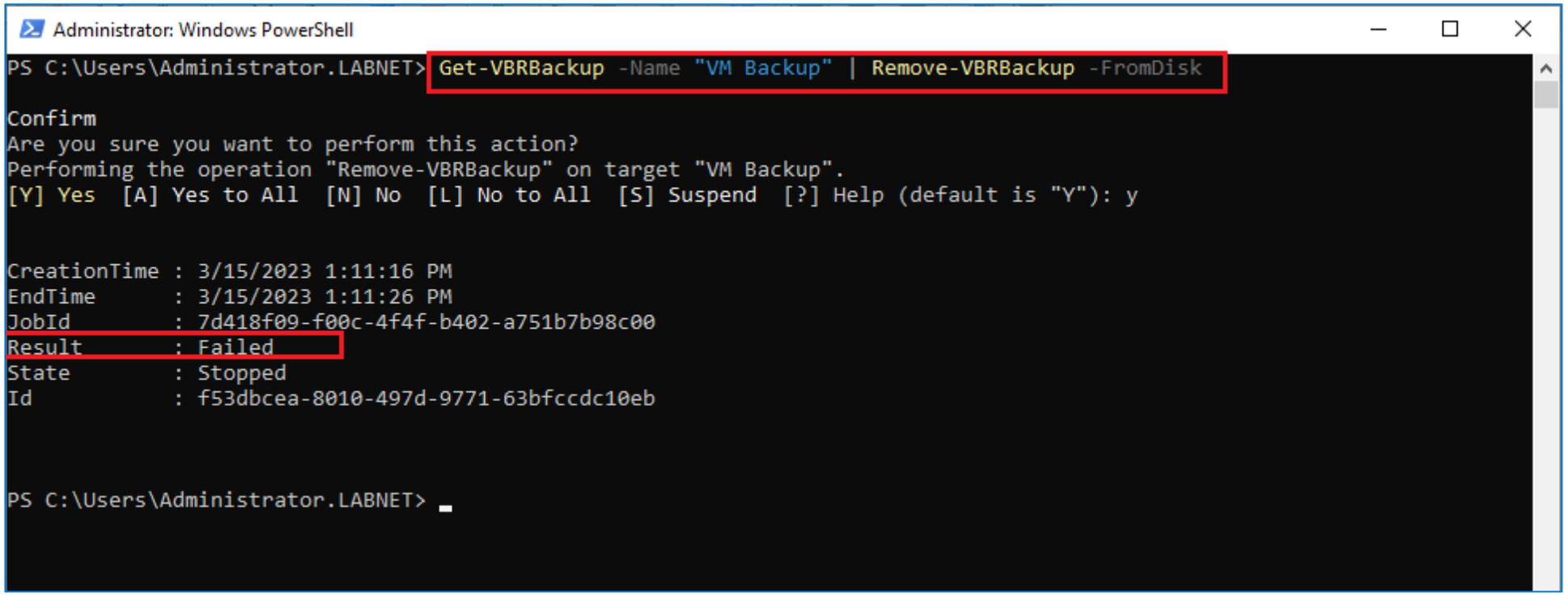
Verificare l'efficacia dell'immutabilità





Verificare l'efficacia dell'immutabilità

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



ICT POWER.IT

Microsoft

Grazie

Raffaele Valensise

Senior Systems Engineer, Veeam Software

raffaele.valensise@veeam.com

@rafvalensise

/rvalensise