



Acronis

Acronis Disaster Recovery

La soluzione Disaster Recovery a portata di mano

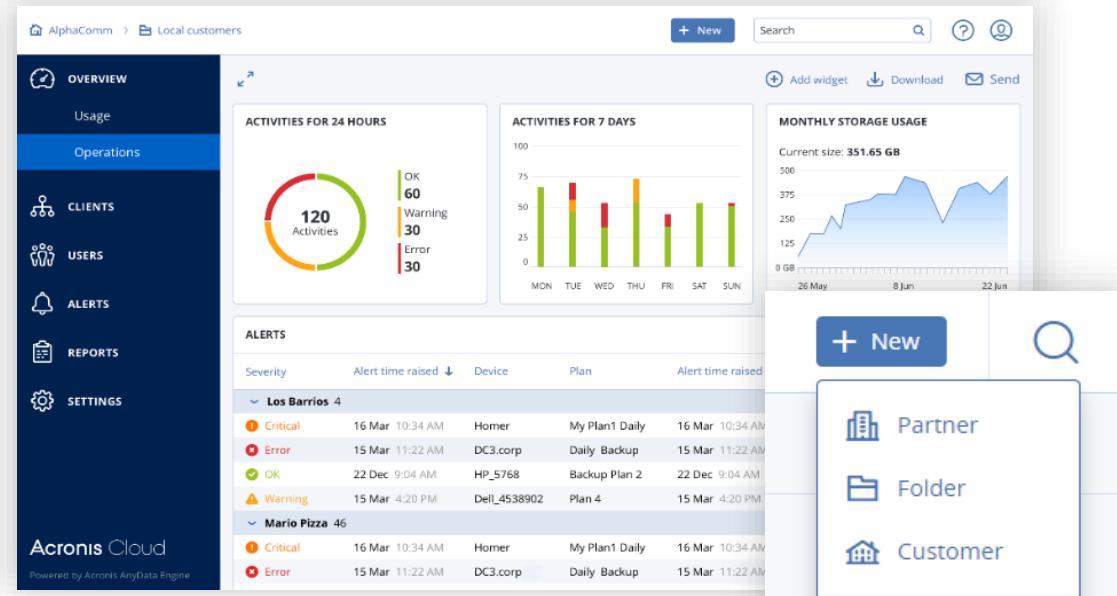
14 Novembre 2025

Webinar

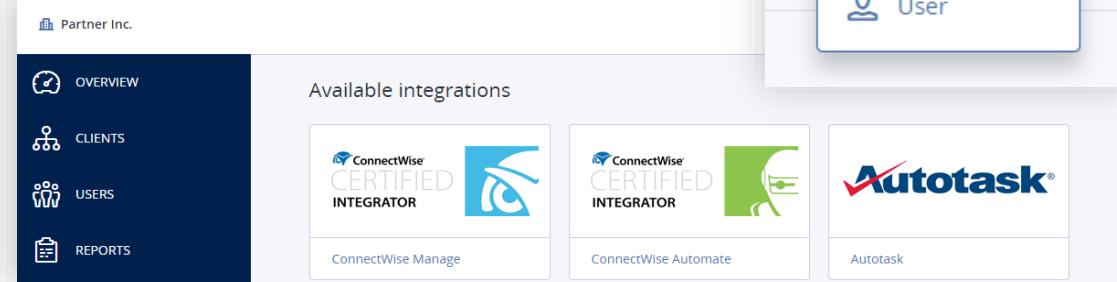
Lorenzo Maraschi – Sales Specialist – TD SYNNEX

Andrea Pezzoni – Security Presales Specialist – TD SYNNEX

La piattaforma pensata per i Service Provider



Acronis Cloud
Powered by Acronis AnyData Engine



Available integrations

- ConnectWise CERTIFIED INTEGRATOR
- ConnectWise CERTIFIED INTEGRATOR
- Autotask

ConnectWise Manage ConnectWise Automate Autotask

Gestione facile e scalabile degli account dei clienti, assicurata da una console web facile da usare (One Console)



Integrazioni con oltre 200 brand di terze parti, PSA, RMM, Cloud Storage e Security



Unico agente per tutte le funzionalità con possibilità di agent-less backup



Personalizzazione del brand (White Label)



Prezzi semplici a consumo (Pay-as-you-Go)

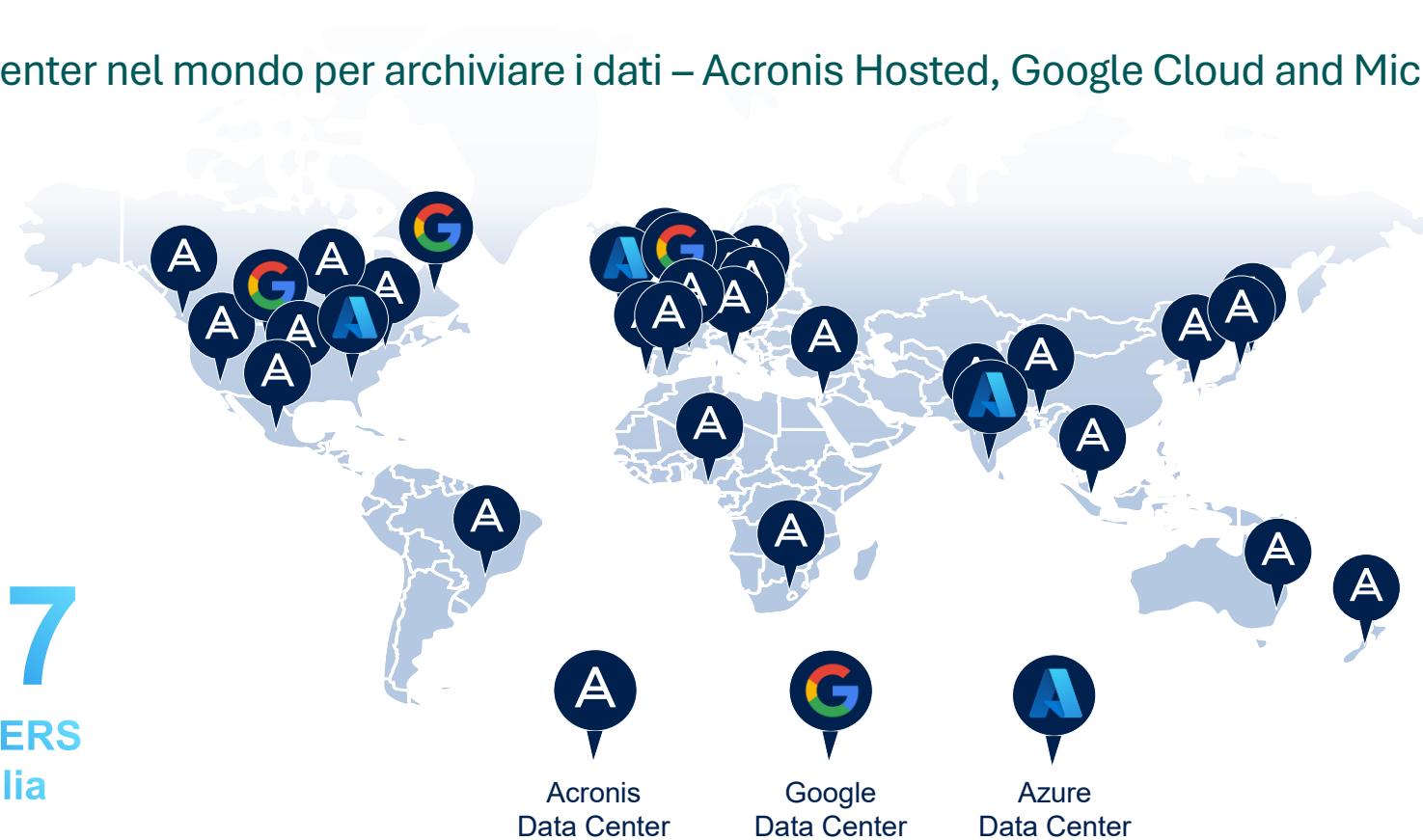


Compliance e presenza locale e globale

Scegli tra oltre 50 data center nel mondo per archiviare i dati – Acronis Hosted, Google Cloud and Microsoft Azure



45+7
DATA CENTERS
Anche in Italia



Soluzioni modulari e licensing semplice

Acronis Cyber Protect Cloud

One platform, one agent, all within one protection plan. Complete coverage of NIST Framework: Govern, Identify, Protect, Detect, Respond and Recover

DATA PROTECTION		CYBERSECURITY		OPERATIONS	
Backup	Disaster Recovery	Detection and Response	SaaS Security	RMM	PSA
Standard Backup <ul style="list-style-type: none"> Backup of 25+ workload types Local and cloud storage Encryption and deduplication Ransomware-proof backup Microsoft 365 <ul style="list-style-type: none"> Exchange Online, SharePoint Online, OneDrive, Teams, OneNote Email Archiving Group management Advanced Backup <ul style="list-style-type: none"> One-click mass recovery Continuous data protection Backup frequency for Microsoft 365 and Google Workspace Off-host validation, replication and conversion to VMs Support for additional workload types Backup notarization 	FREE <ul style="list-style-type: none"> Test failover Cloud-only VPN connection Disaster Recovery <ul style="list-style-type: none"> Production and test failover to Acronis Cloud Orchestration with runbooks AI-assisted, automated test failover Fast, automated fallback with near-zero downtime Multiple connectivity options: <ul style="list-style-type: none"> IPsec Multisite VPN, L2 site-to-site open VPN, cloud-only VPN 	FREE <ul style="list-style-type: none"> AI-based anti-malware protection #CyberFit Score (security posture assessment) Device control Endpoint Detection and Response (EDR) <ul style="list-style-type: none"> Gen AI-guided incident investigation, analysis, automated response Single-click response, including attack-specific rollback and recovery Next-generation antivirus (NGAV) Anti-ransomware protection Zero-day and exploit protection URL filtering Anti-malware scans of backups Extended Detection and Response (XDR) <ul style="list-style-type: none"> Includes all the features of Advanced Security + EDR Extended endpoint protection with visibility and response across most vulnerable attack surfaces: email, identity, Microsoft 365 apps, network Gen AI-guided incident investigation, analysis, response and recovery Managed Detection and Response (MDR) <ul style="list-style-type: none"> 24/7/365 Continuous monitoring with expedited investigation from security analysts Event triage, prioritization and rapid response including recovery Data Loss Prevention (DLP) <ul style="list-style-type: none"> Control sensitive data transfers across local and network channels Prebuild data classifiers for common regulatory frameworks Automatic client-specific DLP policy creation and extension 	Email Security <ul style="list-style-type: none"> Phishing and Quishing prevention Business Email Compromise prevention Malware protection APT and zero-day protection Account takeover detection Incident response service Microsoft 365, Google Workspace, Exchange and any SMTP supporting email service Collaboration Security <ul style="list-style-type: none"> Microsoft 365 SharePoint, OneDrive and Teams security protection Malware protection APT and zero-day protection Incident response service Security Posture Management for Microsoft 365 <ul style="list-style-type: none"> Continuous monitoring of security posture Automatic and manual remediation of risks Microsoft 365 user offboarding Security Awareness Training <ul style="list-style-type: none"> Rich and engaging library of training courses Phishing simulation and exercises Mobile-friendly learning experience Available in multiple major languages 	FREE <ul style="list-style-type: none"> Endpoints <ul style="list-style-type: none"> Device Sense™ device discovery Hardware inventory Vulnerability assessments Remote desktop (RDP) Microsoft 365 <ul style="list-style-type: none"> Multitenant Microsoft 365 management Security posture baselines On-demand security audits Microsoft 365 user onboarding Remote Management and Monitoring (RMM) for endpoints <ul style="list-style-type: none"> Vulnerability assessments (third-party apps) AI-assisted patch management Fail-safe patching DeployPilot™ for AI-enhanced software deployment ML-based monitoring Auto-response actions AI-enabled remote scripting Remote desktop and assistance: advanced features Geolocation tracking for devices Software inventory 	Professional Services Automation (PSA) <ul style="list-style-type: none"> Billing and invoicing Service desk Time tracking Contracts and quotes Project management Stock inventory management KPI reporting

L'interruzione dell'attività è un rischio concreto



40%

Percentuale di aziende SMB
che hanno riportato una
perdita di dati a seguito di
un Cyber Attack



43%

Delle aziende SMB non ha
un piano di remediation per
ripartire dopo un incidente
informatico



60%

Le organizzazioni del segmento
Small che sono
costrette a chiudere entro
6 mesi da un attacco informatico



82%

Gli attacchi rivolti alle SMB

Acronis DR: prezioso per gli MSP



Meno interruzioni

Rendete operativi i clienti in pochi minuti avviando i sistemi IT in Acronis Cloud e sfruttate la connettività site-to-site completa e la possibilità di ripristinare i sistemi su hardware simile o diverso.



Riduci al minimo la complessità

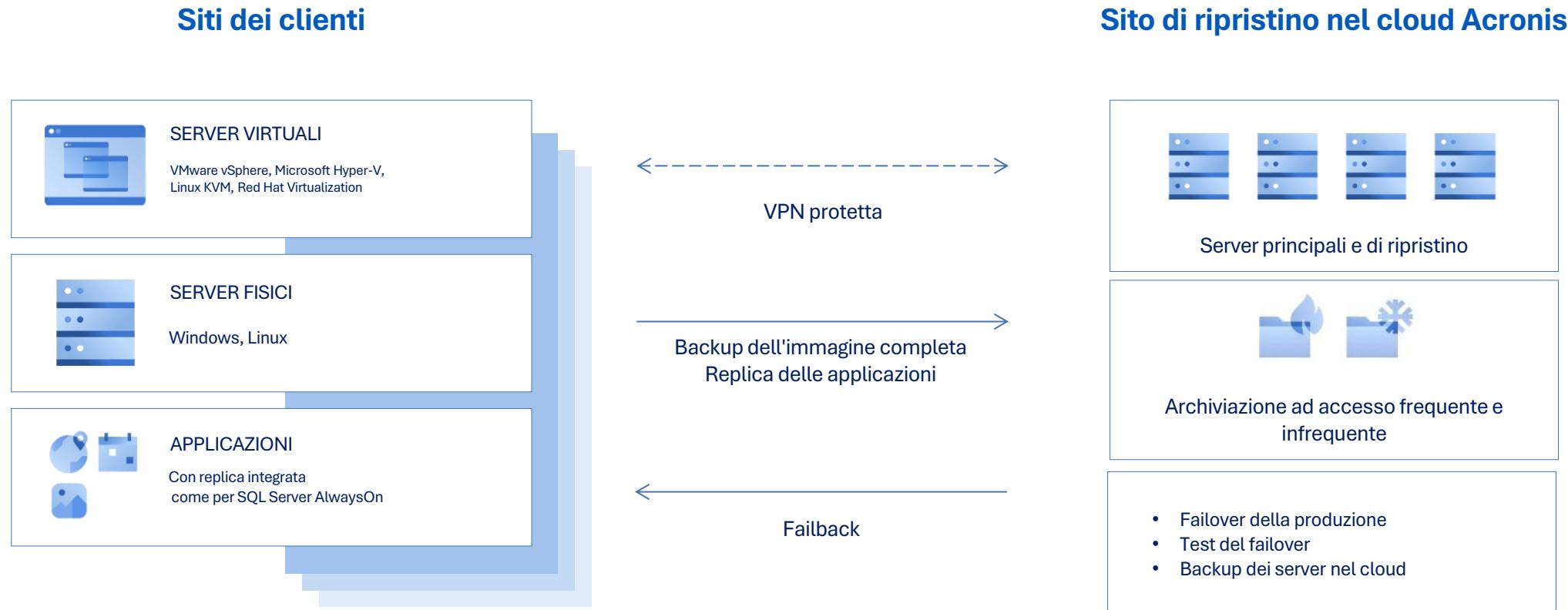
Non c'è bisogno di aggiungere, imparare a usare o gestire un'altra piattaforma. È un'unica soluzione per qualsiasi workload, gestita da un'unica interfaccia che consente di creare un servizio di cyber protection completo.



Fai crescere il reddito ricorrente

Offrite più valore, rafforzate le relazioni con i clienti e aumentatene la fidelizzazione fornendo loro i servizi di disaster recovery di cui hanno bisogno, aumentando al contempo gli utili mensili ricorrenti.

DR in Acronis Cloud



DR senza limiti

Sistemi fisici e virtual machine

Piattaforme di virtualizzazione

Server nel cloud per la replica delle applicazioni in tempo reale

Windows

- VMware vSphere
- Microsoft Hyper-V
- Linux KVM

Linux

- Red Hat Virtualization
- Citrix XenServer



Server Windows

Exchange

SQL Server

Share Point

Active Directory

Hyper-V



Citrix XenServer



Server Linux



VMware vSphere



Virtualizzazione Red Hat



Linux KVM

Acronis

Comprehensive built-in features

A
NIS2

Business Mgmt.		Backup and Disaster Recovery						Cybersecurity																					
Icon	Feature	Icon	Feature	Icon	Feature	Icon	Feature	Icon	Feature	Icon	Feature	Icon	Feature																
	Remote Monitoring Access (RMM)		Patch Management		Trad. Backup		Backup as a service		Archive as a service		Disaster Recovery as a service		Data visibility		Data Loss Prevention		Incident investigation		Ransomware protection		Vulnerability assessment		Detection & response		Endpoint protection		Malware Resistance		Messaging Security

NIS 2: Obblighi per le aziende

Gestione del rischio

La direttiva NIS2 dell'Unione Europea richiede alle organizzazioni di dimostrare un piano di disaster recovery per garantire la continuità operativa in caso di incidenti gravi.

Obblighi di comunicazione

Implementare una soluzione di disaster recovery come quella offerta da Acronis Cyber Protect Cloud aiuta le organizzazioni a conformarsi a questi requisiti, migliorando la loro resilienza contro le minacce informatiche.

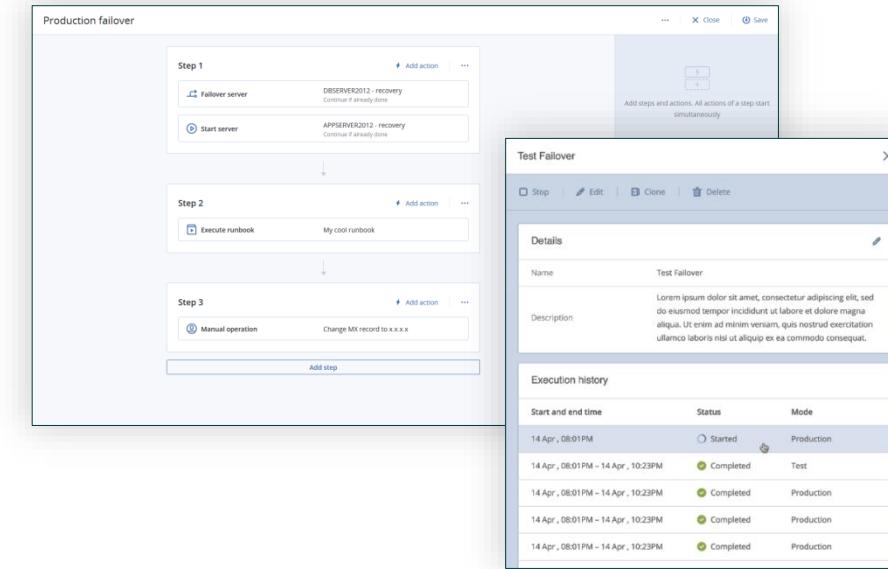
Business Continuity

I vantaggi del DR di Acronis

Migliora gli RTO e automatizza il disaster recovery con i runbook

La funzione runbook semplifica e velocizza il failover di più dispositivi su un sito di ripristino su cloud.

Consente di automatizzare in modo efficiente il failover e i test e garantisce il ripristino dei sistemi nell'ordine giusto per mantenere le interdipendenze tra applicazioni su dispositivi diversi.



Perché? Garantisce che tutti i sistemi vengano ripristinati nell'ordine giusto

Acronis

Automatizza il fallback

Ottieni i tempi di fallback migliori del settore e proteggi i dati dei clienti trasferendoli sul sito locale mentre la virtual machine è in esecuzione nel cloud. Ricevi aggiornamenti sullo stato del sistema e ottieni stime della durata prevista dell'interruzione dell'attività per pianificare efficacemente il processo di fallback.

Ottimizza il lavoro gestendo

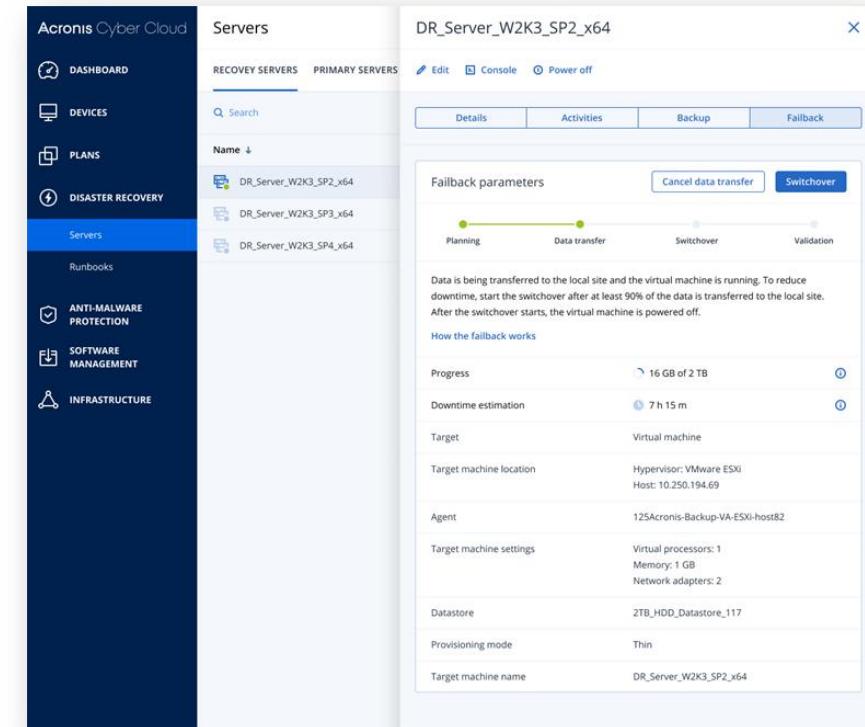
l'intero processo in un'unica schermata

Approfitta dei tempi di

interruzione operativa per il ripristino più bassi sul mercato

Evita confusione con semplici

istruzioni per l'utente in interfaccia



Perché?

Riduci quasi a zero i tempi morti, garantisci la continuità operativa e proteggi i dati dei tuoi clienti

Acronis

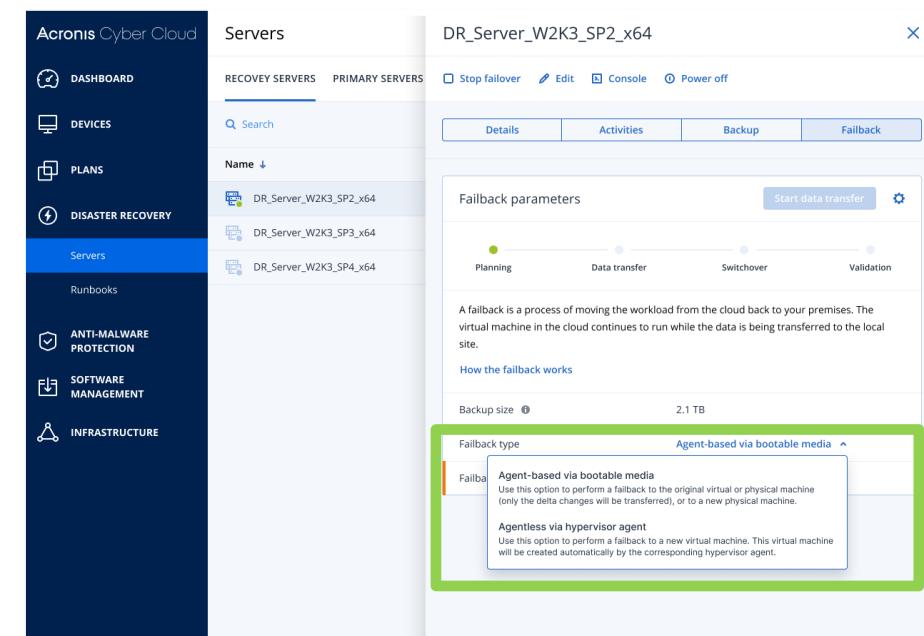
Fallback rapido

Ora è possibile eseguire un fallback incrementale rapido direttamente sulla macchina virtuale originale tramite l'agente Acronis, trasferendo solo le modifiche delta e non l'intera immagine della VM.

- **Fallback fino a 3 volte più veloce:** grazie al fallback incrementale, dalla memoria Acronis Cloud alla macchina originale vengono trasferite solo le modifiche delta.
- **Interruzioni operative ridotte al minimo durante il fallback:** la VM nel cloud continua a funzionare durante il trasferimento dei dati, garantendo che l'intero processo di fallback sia fluido e con interruzioni operative ridotte al minimo.
- **Complessità ridotta:** evita la configurazione di una nuova macchina e l'uso di un hypervisor per il fallback.

Scenari

- **Con agente, tramite supporto di avvio:** esegui il fallback sulla macchina fisica o virtuale di origine (vengono trasferite solo le modifiche delta) oppure su una nuova macchina fisica.
- **Senza agente, tramite agente hypervisor:** esegui il fallback su una macchina virtuale. Questa macchina virtuale verrà creata automaticamente dall'agente corrispondente dell'hypervisor.
- Fallback rapido disponibile per macchine fisiche e virtuali.

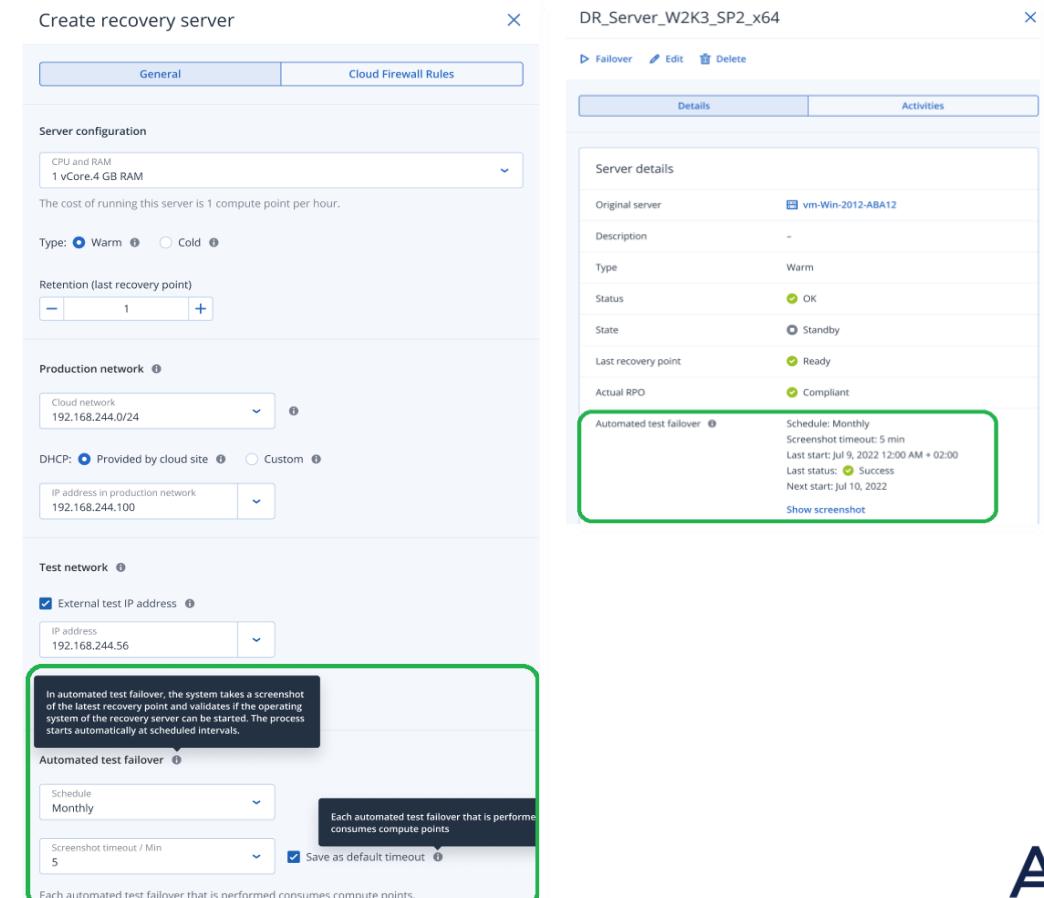


Failover di prova

Risparmia tempo e lavoro con un test di failover semplificato e automatizzato.

Con il pacchetto Disaster Recovery Advanced puoi eseguire test di failover automatizzati pianificati per qualsiasi server, con la certezza di poter poi ottenere ripristini rapidi e affidabili.

- La verifica tramite screenshot basata su intelligenza artificiale consente di verificare che i workload siano attivi e in esecuzione nel cloud
- Dopo ogni sessione di test viene creato un report di consolidamento con i dettagli del test per ogni workload



Create recovery server

DR_Server_W2K3_SP2_x64

Automated test failover

The screenshot displays two windows from the Acronis Disaster Recovery Advanced software. The left window, titled 'Create recovery server', shows configuration for a new server, including 'Server configuration' (CPU and RAM), 'Production network' (Cloud network set to 192.168.244.0/24), and 'Test network' (External test IP address set to 192.168.244.56). A callout box highlights the 'Automated test failover' section at the bottom, which includes a schedule of 'Monthly', a screenshot timeout of '5 min', and a checkbox for 'Save as default timeout'. The right window, titled 'DR_Server_W2K3_SP2_x64', shows details for an existing server, including its original server (vm-Win-2012-ABA12), status (OK, Standby), and last recovery point (Ready). It also shows an 'Automated test failover' section with a history of runs, including the most recent one on Jul 10, 2022, which was successful. A green box highlights this section.

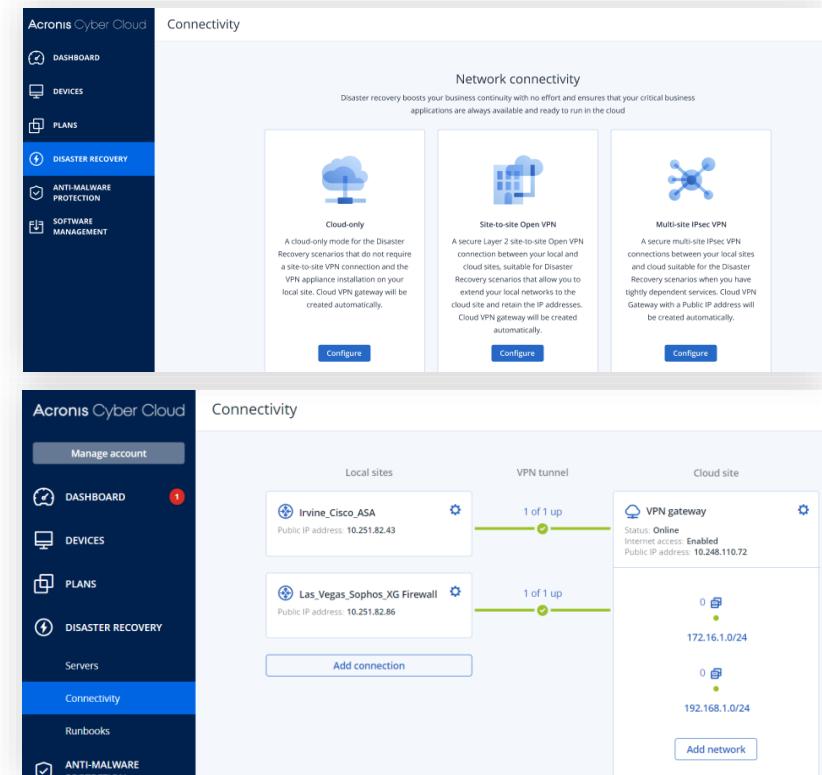
IpSec Multisito

Supporto per VPN IPsec multisito

Rafforza la sicurezza per i tuoi clienti

Integra protocolli e algoritmi sicuri, per supportare facilmente i clienti con più siti che ospitano workload critici e con requisiti più elevati in termini di sicurezza, conformità e larghezza di banda.

Stato trasparente delle connessioni e dei tunnel e risoluzione automatica dei problemi.



Perché? Supporta facilmente i clienti con più siti che ospitano workload critici

Acronis

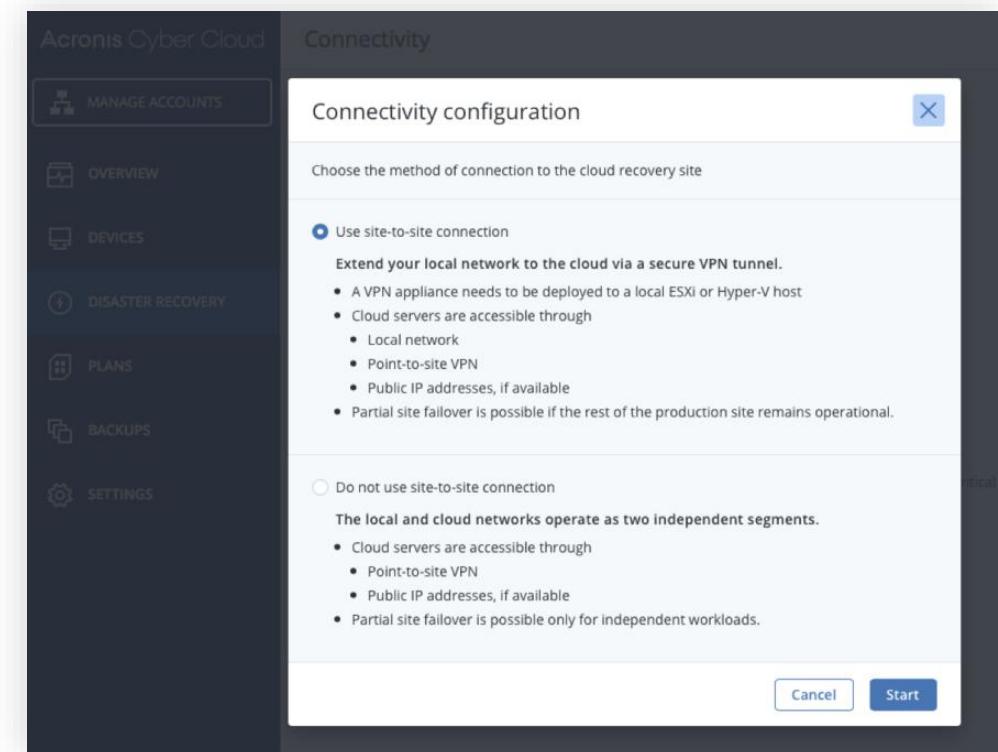
Deployment senza VPN

Esegui l'onboarding dei clienti in modo più semplice e rapido

L'appliance virtuale VPN non è necessaria per la connettività "point-to-site".

Passaggio in qualsiasi momento dalla modalità "da punto a sito" a quella "da sito a sito".

Questa opzione è utile soprattutto per i clienti che desiderano valutare velocemente il servizio o che non hanno l'esigenza di estendere la rete locale al sito cloud.



Perché? Offri ai clienti opzioni rapide e semplici di connettività da punto a sito o da sito a sito

Acronis

Ripristini sicuri

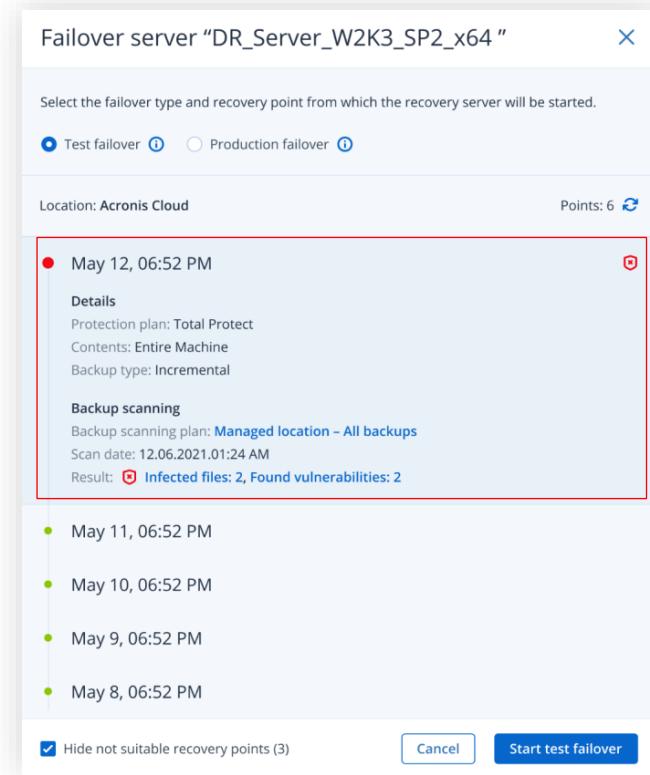
Failover su un punto di ripristino privo di malware

Adozione di un atteggiamento proattivo per evitare la reinfezione

Controlla l'elenco dei punti di ripristino disponibili per il failover per verificare se durante il processo di scansione del backup è stato rilevato un malware o un altro indicatore di compromissione.*

Garantisce un ritorno più rapido e sicuro alla produttività prevenendo la reinfezione dovuta a un punto di ripristino compromesso.

* Per eseguire la scansione anti-malware dei backup è necessario abilitare Advanced Security.

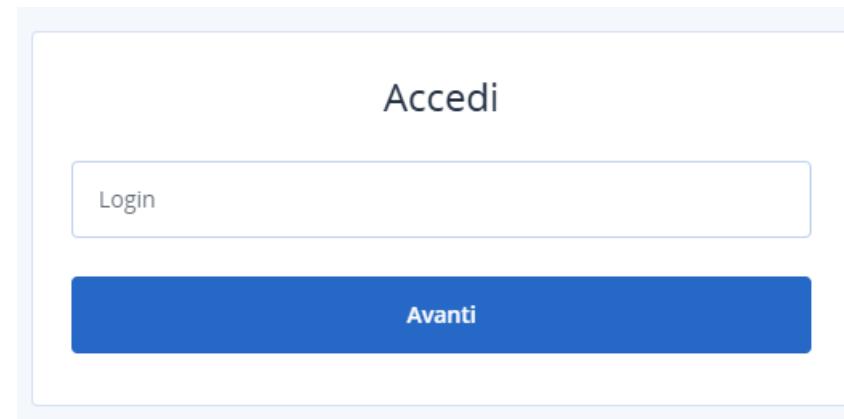


Perché? Per garantire la riuscita del ripristino selezionando punti di ripristino privi di malware

Acronis

Hands-on

Acronis



“The key to an effective recovery plan is to rely on the public cloud, not your own datacenter or hardware.”

Poojan Kumar

<https://www.acronis.com/it-it/solutions/disaster-recovery/>

<https://www.acronis.com/it-it/products/cloud/cyber-protect/disaster-recovery>

<https://www.acronis.com/it-it/blog/tags/disaster-recovery/>

<https://www.acronis.com/it-it/>

<https://nis2directive.eu/>

<https://www.packetlabs.net/posts/the-top-cybersecurity-statistics-for-2024/>

Q&A

PROSSIMI APPUNTAMENTI

21 NOVEMBRE: Airbus Security

28 NOVEMBRE: Sonicwall MPSS

<https://events.tdsynnex.it/cyber-unit-missione-protezione/>

TEAM SECURITY: security.it@tdsynnex.com

SPEAKER: andrea.pezzoni@tdsynnex.com
lorenzo.maraschi@tdsynnex.com