

Acronis Cyber Foundation

Program

Transformer des vies grâce à l'éducation

Unissons nos efforts pour créer de nouvelles connaissances en mettant la diversité de nos expériences et de nos points forts au service d'un avenir plus radieux.



Rejoignez-nous !



Acronis

#CyberFit

Acronis Cyber Cloud Le PRA avec Acronis Cloud



Grégory Laroche
Senior Solution Engineer

Votre Webinaire commence dans 1mn

Acronis

#CyberFit

Acronis Cyber Cloud Le PRA avec Acronis Cloud



Grégory Laroche
Senior Solution Engineer

BIENVENUE !

Acronis, leader de la cyberprotection

Cyberprotection pilotée par l'intelligence artificielle, Cyber Cloud, Cyber Platform



Suisse

Siège social à Schaffhausen
(Suisse) depuis 2008

Singapour

Fondée à Singapour en 2003,
siège international actuel

Deux sièges sociaux pour une double protection



Croissance et développement

- +300 millions de dollars de CA
- Croissance des activités de 50 %
- +100% de croissance des activités cloud
- 100 % des entreprises Fortune 1000
- +1 000 000 entreprises
- +50 000 partenaires



Présence mondiale

- +2 500 collaborateurs
- +33 bureaux
- +150 pays
- +33 langues
- 50 Datacenters dans le monde



304 régions d'information de vol

Acronis Cyber Protect

- +2 000 000 ressources protégées
- +2 000 000 attaques évitées
- +16 000 partenaires cloud



Sauvegarde de pointe

avec sécurité et gestion intégrées

PROTECTION INNOVANTE

Acronis Cyber Protect Cloud

SÉCURITÉ

- Score #CyberFit
- Évaluation des vulnérabilités
- Protection contre les ransomwares
- Protection antivirus et anti-malware sans détection basée sur les signatures locales
- Contrôle des terminaux

NOTARISATION (FACTURATION À L'UTILISATION)

GESTION

- Gestion de groupes de ressources
- Gestion des plans centralisés
- Bureau à distance
- Assistance à distance
- Inventaire des matériels



Ressource

SAUVEGARDE

(FACTURATION À L'UTILISATION)

- Sauvegarde de fichiers
- Sauvegarde d'images
- Sauvegarde d'applications
- Sauvegarde de partages réseau
- Sauvegarde dans le cloud
- Sauvegarde en local

REPRISE D'ACTIVITÉ APRÈS SINISTRE

- Tests de basculement
- Connexion VPN cloud uniquement

SYNCHRONISATION ET PARTAGE DE FICHIERS (FACTURATION À L'UTILISATION)

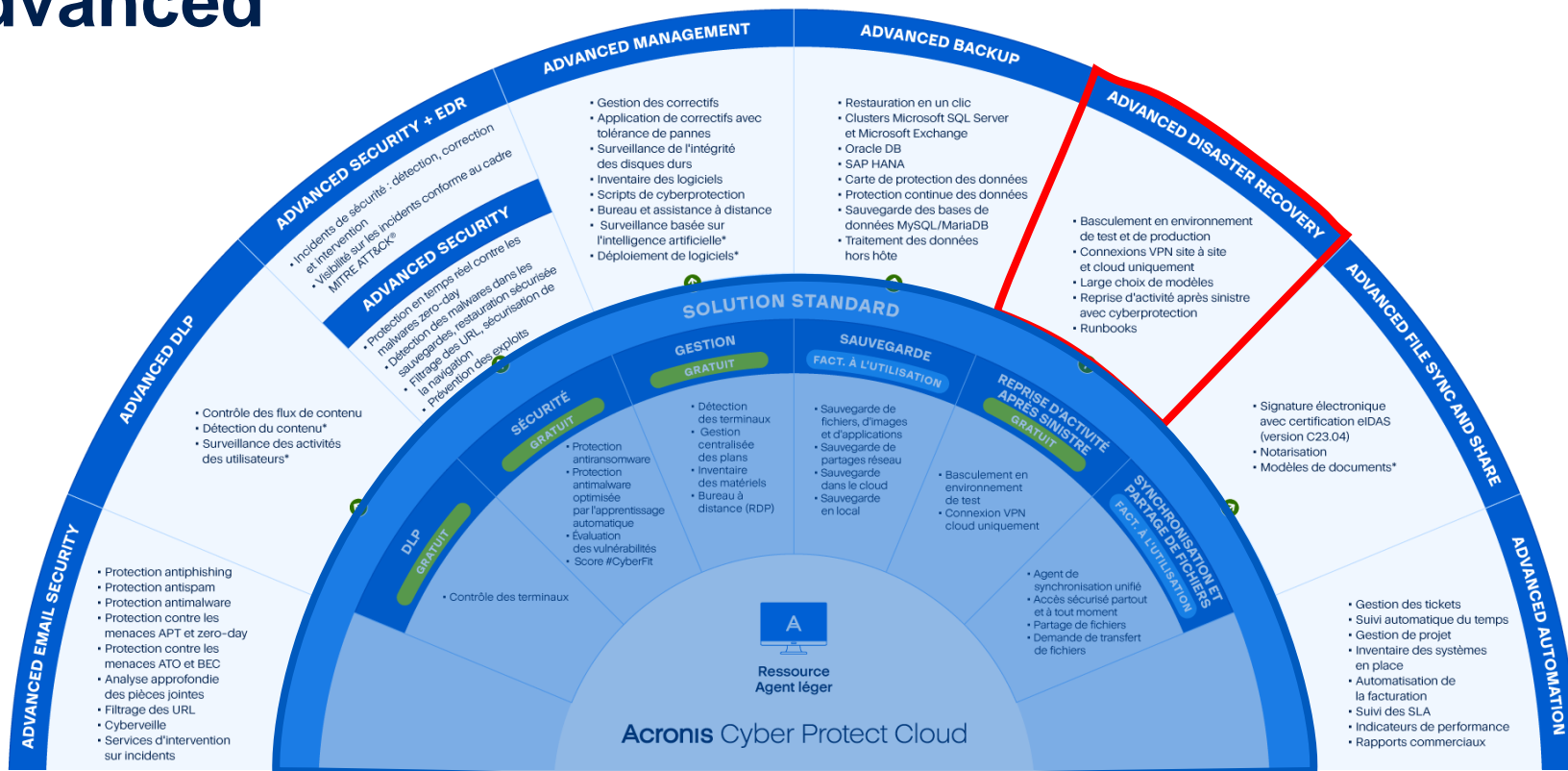
Protection de toutes les ressources, sans frais

Sauvegarde de pointe incluse

Protection renforcée contre les menaces zero-day

Sécurité et gestion accélérées

Acronis Cyber Protect Cloud associé aux packs Advanced



Le nouveau monde des menaces



Catastrophes naturelles

- Seulement **6 %** des pannes sont dues à des catastrophes naturelles(1)
- Affecte les installations et les infrastructures



Pandémies

- Nécessite un scénario de **planification différent**
- Affecte les personnes



Défaillance du matériel, corruption du logiciel

Jusqu'à 30 millions de PME sont vulnérables aux pannes informatiques en **l'absence d'une surveillance complète**(2)



Suppression accidentelle de données

14% des pertes de données sont dues à des **erreurs humaines**, telles que la suppression ou l'écrasement de fichiers(3).



Cyberattaques

- **93 %** des entreprises ont été attaquées au cours des **trois dernières années**(2)
- Les attaques de **logiciels malveillants** ont augmenté de **25 %**(4)
- D'ici 2021, la cybercriminalité coûtera **6 000 milliards de dollars** par an(4)

Natural

Human

Les clients ne peuvent pas se permettre des temps d'arrêt

40%

des entreprises **ont subi une violation de données** en 2020

8000€

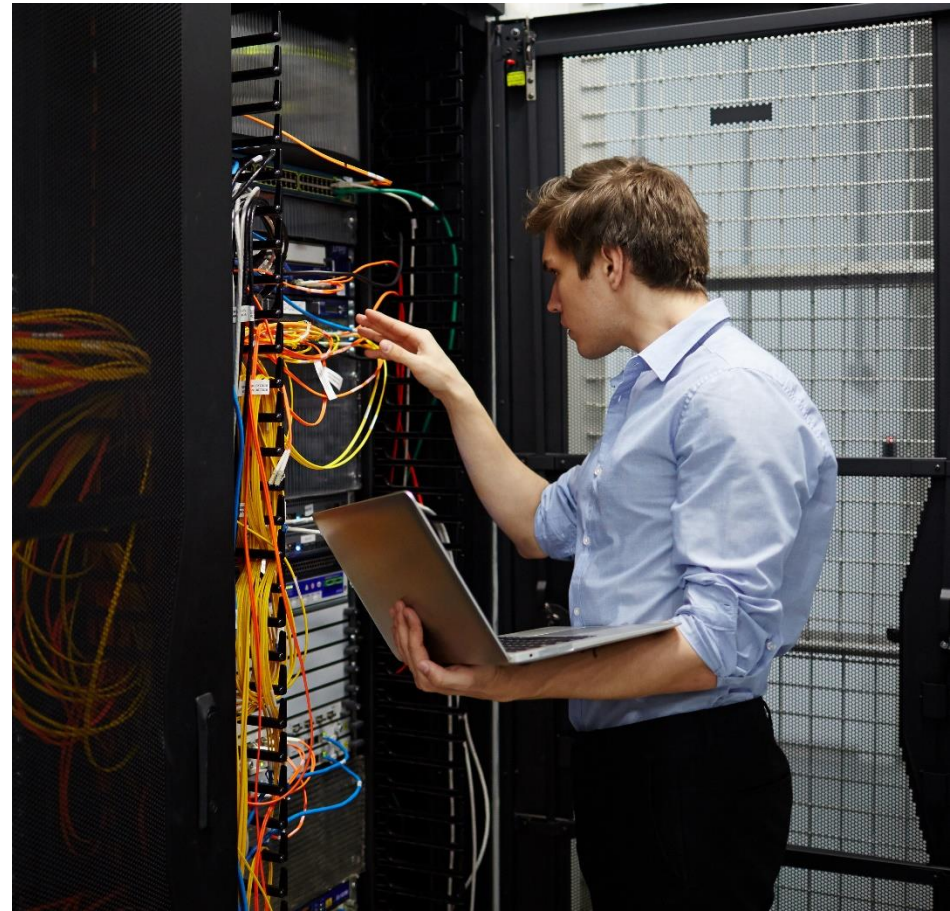
coût horaire moyen **d'un temps d'arrêt non planifié** pour une PME

14 heures

temps d'arrêt **annuel moyen** pour les entreprises

545 heures

le nombre annuel moyen d'heures de **perte de productivité du personnel**



La reprise après sinistre a évolué



1990s



2000s



2010s

Centre de données de l'entreprise ou cage de colocation

- Matériel à amortir
- Mise en réseau
- Licences
- Plateformes de réplication
- Quantités massives de stockage

Approche hybride

- Des licences coûteuses
- Compliqué
- Couverture limitée

DR hybride moderne et basé sur le cloud

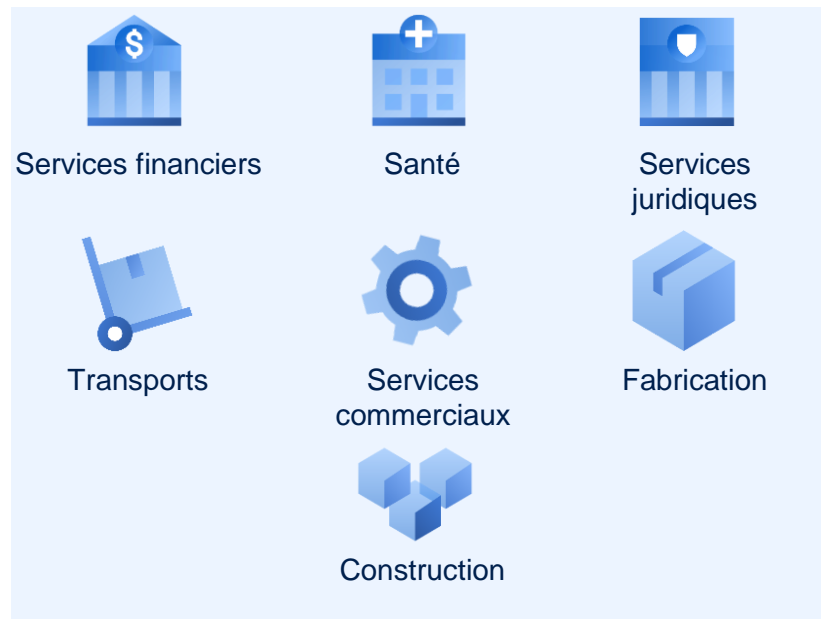
- Rentabilité
- Facilité d'utilisation
- Prêt à l'emploi

Qui a besoin d'une solution de reprise d'activité après sinistre ?

Les entreprises qui :

- s'appuient sur des applications et des données **stratégiques**
- sont soumises à des **exigences de conformité** réglementées
- sont partenaires dans des **chaînes logistiques exigeantes**
- sont établies dans des **zones exposées aux sinistres**
- **manquent de ressources** techniques
- **dépendent fortement de l'informatique**

Secteurs clés :



Acronis

#CyberFit

PRA dans le Cloud Acronis : Principaux avantages.

Une intégration poussée permet de nouvelles capacités

Intégration à tous les niveaux : gestion, produits, technologie

Exploiter la puissance de l'unification :

- Éliminer la complexité
- Fournir de nouvelles capacités de sécurité
- Réduire les coûts
- Gérer tous les clients à partir d'une seule console
- escalade efficace de l'assistance avec un seul fournisseur

One

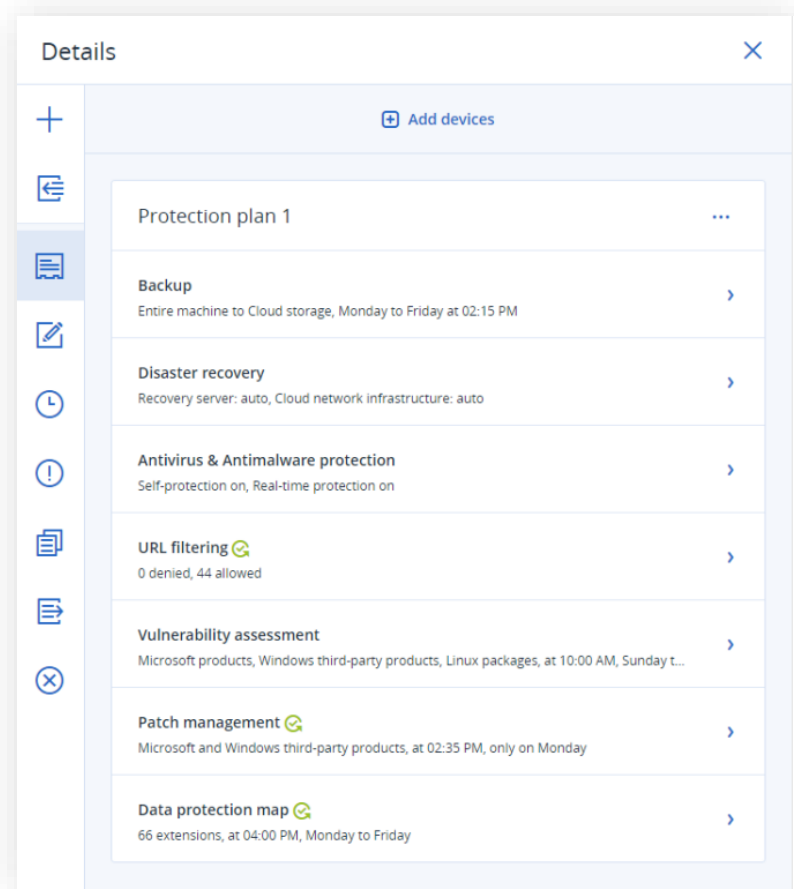
Agent

● Policy

● UX/UI

● License

● Vendor



Acronis Cyber Protect Cloud with Advanced Disaster Recovery



Moins de temps d'arrêt des services

Faites fonctionner les clients en quelques minutes en faisant tourner les systèmes informatiques dans le nuage Acronis avec une connectivité complète de site à site et la possibilité de les restaurer sur du matériel similaire ou différent.



Minimiser la complexité

Pas besoin d'ajouter, d'apprendre ou de gérer une autre plateforme. Il s'agit d'une solution unique pour toutes les charges de travail, gérée à partir d'une interface unique, qui vous permet de mettre en place un service complet de cyberprotection.



Augmenter les revenus récurrents

Apportez plus de valeur ajoutée, approfondissez les relations avec vos clients et fidélisez-les en leur offrant les services de reprise après sinistre qu'ils recherchent, tout en augmentant vos revenus mensuels récurrents..

Simplification de la reprise d'activité après sinistre des clients grâce à une solution SaaS clé en main



Reprise d'activité après sinistre pour les ressources **virtuelles et physiques**



Réplication des machines de production **basée sur les sauvegardes**



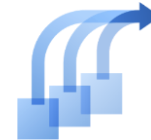
Orchestration de la reprise d'activité après sinistre à l'aide de runbooks



Extension aisée des réseaux locaux au site de restauration cloud



Tests de basculement dans des environnements isolés, sans interruption d'activité



Plusieurs points de restauration

Acronis

#CyberFit

Connectivité réseau :
Simple sans être simpliste.

VPN Point a site : Option de déploiement sans VPN coté client

Intégration plus simple et rapide des nouveaux clients

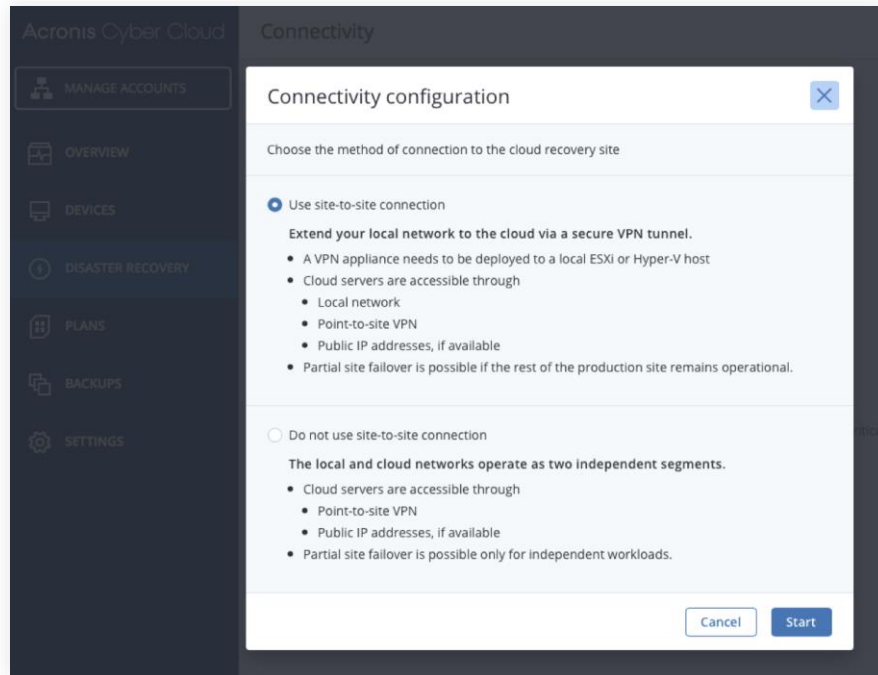
L'appliance virtuelle VPN n'est pas nécessaire pour la connectivité « point-à-site ».

Passez du mode « point-à-site » au mode « site-à-site » selon ce qui vous convient.

Cette option est particulièrement utile pour les clients qui souhaitent évaluer rapidement le service ou qui n'ont pas besoin d'étendre le réseau local au site cloud.

Pourquoi ?

Connexion simple et rapide des clients grâce à la connectivité point-à-site ou site-à-site



VPN Site a site : Prise en charge de plusieurs réseaux

Prise en charge d'infrastructures clients plus complexes

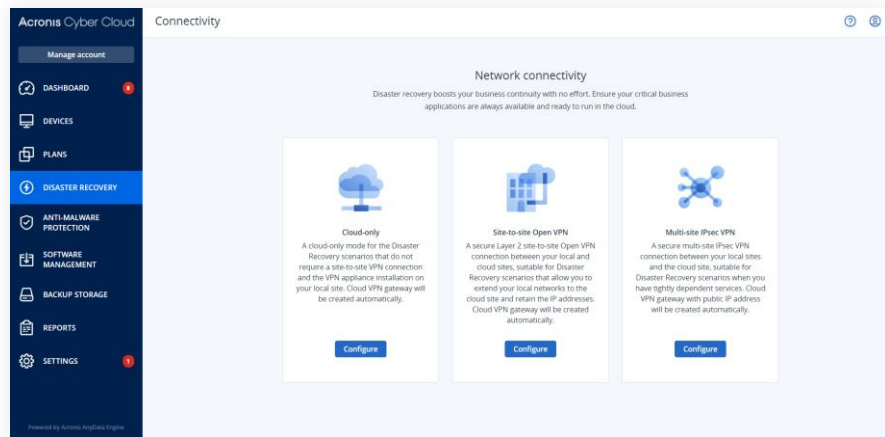
Vous pouvez facilement étendre jusqu'à cinq réseaux locaux au site de restauration cloud d'Acronis au moyen de la connexion site-à-site.

Basculez des environnements complexes au sein desquels les serveurs protégés sont répartis sur plusieurs segments réseau.

Identifiez les états de connectivité des cinq réseaux en un coup d'œil.

Pourquoi ?

Support de différents types de clients grâce à la prise en charge d'infrastructures plus complexes



Prise en charge des VPN multisites : IPsec

Renforcement de la sécurité de vos clients

La prise en charge des VPN multisites IPsec intègre des algorithmes et protocoles sécurisés vous permettant de supporter les clients disposant de plusieurs sites qui hébergent des ressources critiques soumises à des exigences plus strictes en matière de sécurité, de conformité et de bande passante.

État transparent des connexions et des tunnels et autodépannage

Pourquoi ?

Support aisé des clients disposant de plusieurs sites qui hébergent des ressources critiques

The image displays two screenshots of the Acronis Cyber Cloud interface. The top screenshot shows the 'Connectivity' page with three options: 'Cloud-only', 'Site-to-site Open VPN', and 'Multi-site IPsec VPN'. The bottom screenshot shows a detailed view of a VPN tunnel configuration, including local sites (Irvine_Cisco_ASA and Las_Vegas_Sophos_XG Firewall) and a cloud site (VPN gateway).

Acronis Cyber Cloud Connectivity

Network connectivity
Disaster recovery boosts your business continuity with no effort and ensures that your critical business applications are always available and ready to run in the cloud.

- Cloud-only**
A cloud-only mode for the Disaster Recovery scenarios that do not require a site-to-site VPN connection and the VPN appliance installation on your local site. Cloud VPN gateway will be created automatically.
- Site-to-site Open VPN**
A secure Layer 2 site-to-site Open VPN connection between your local and cloud sites, suitable for Disaster Recovery scenarios that allow you to extend your local networks to the cloud site and retain the IP addresses. Cloud VPN gateway will be created automatically.
- Multi-site IPsec VPN**
A secure multi-site IPsec VPN connections between your local sites and cloud suitable for the Disaster Recovery scenarios when you have highly dependent services. Cloud VPN Gateway with a Public IP address will be created automatically.

Acronis Cyber Cloud Connectivity

Local sites

- Irvine_Cisco_ASA
Public IP address: 10.251.82.43
- Las_Vegas_Sophos_XG Firewall
Public IP address: 10.251.82.86

VPN tunnel

- 1 of 1 up
- 1 of 1 up

Cloud site

- VPN gateway**
- Status: Online
- Internet access: Enabled
- Public IP address: 10.248.110.72
- 0 servers
- 172.16.1.0/24
- 0 servers
- 192.168.1.0/24

Acronis

#CyberFit

Automatisation des workloads l'orchestration avec les Runbooks

Réduction des RTO et automatisation de la reprise d'activité après sinistre à l'aide de runbooks

- Les runbooks simplifient et accélèrent le basculement de plusieurs machines vers un site de restauration cloud.
- Cette fonction renforce l'efficacité des opérations d'automatisation du basculement et des tests. De plus, elle s'assure que les systèmes sont restaurés dans le bon ordre afin de respecter les interdépendances entre les applications sur différentes machines.

The screenshot displays the Acronis Runbook interface. The main window, titled 'Production failover', shows a sequence of three steps:

- Step 1:** Contains two actions: 'Failover server' (DESERVER2012 - recovery) and 'Start server' (APPSERVER2012 - recovery).
- Step 2:** Contains one action: 'Execute runbook' (My cool runbook).
- Step 3:** Contains one action: 'Manual operation' (Change MX record to x.x.x).

A modal window titled 'Test Failover' is open in the foreground, showing details and execution history.

Test Failover Details:

- Name: Test Failover
- Description: Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat.

Test Failover Execution history:

Start and end time	Status	Mode
14 Apr, 08:01 PM	Started	Production
14 Apr, 08:01 PM - 14 Apr, 10:23 PM	Completed	Test
14 Apr, 08:01 PM - 14 Apr, 10:23 PM	Completed	Production
14 Apr, 08:01 PM - 14 Apr, 10:23 PM	Completed	Production
14 Apr, 08:01 PM - 14 Apr, 10:23 PM	Completed	Production

Pourquoi ?

Garantie que tous les systèmes sont restaurés dans le bon ordre

Acronis

#CyberFit

PRA Acronis : La sécurité des assets

Prise en charge des sauvegardes chiffrées

Respect des exigences en matière de sécurité des données

Effectuez un basculement à l'aide de sauvegardes chiffrées et autorisez le système à utiliser les mots de passe stockés dans un emplacement sécurisé pour les opérations de reprise d'activité après sinistre automatisées.

La nouvelle fonctionnalité « Credential Store » (Magasin d'identifiants), accessible à partir de l'onglet « Disaster Recovery » > « Credential Store » (Reprise après sinistre > Magasin d'identifiants), permet de stocker et de gérer en toute sécurité les mots de passe des sauvegardes de serveur chiffrées.




Vous assurez ainsi votre conformité à diverses réglementations en matière de données.

Pourquoi ?

Protection des données clients et conformité à diverses réglementations en matière de données

Encrypted backup passwords

Provide the encryption passwords for the backups of the original server. The passwords are stored in a secure storage.
If you do not provide a password for a backup, automated disaster recovery operations for this backup will not be available.

Backup name	Password	Credential name
 DBSERVER2012 - Backup to cloud 1 RECENT	<input type="password"/>	<input type="text" value="New archive password"/>
 DBSERVER2012 - Backup to cloud 2	<input type="password"/>	<input type="text" value="Saved archive password"/>
 DBSERVER2012 - Backup to cloud 3	<input type="password"/>	<input type="text"/>

Saved archive password 1

Saved archive password 2

Saved archive password 3







Show all backups

Suivi du respect des RPO des serveurs de restauration (SLA)

Meilleur respect des accords de niveau de service (SLA)

Définissez des seuils de point de reprise pour les serveurs de restauration afin de déterminer la date d'ancienneté requise de la sauvegarde cloud de la machine d'origine, à des fins de basculement.

Surveillez le respect des objectifs de point de reprise (RPO) en temps réel via la console Web.

Name ↑	Status	State	RPO compliance
 Server_W2K3_SP2_x64	✓ OK	Test failover	● Compliant
 finance08-Recovery	🔄 In progress...	Recovering...	● Compliant
 fserver	⚠ RPO exceeded	Failover	● Exceeded (1.3x)
 Servier RGYD6	✓ OK	Standby	-
 Server_W2K8x64_SQL	✓ OK	Ready for failback	● Compliant
 fserver	✓ OK	Running	● Compliant

Pourquoi ?

Établissement de SLA compétitifs que vous êtes en mesure de respecter

Basculement automatisé de test

Gagnez du temps et de l'énergie grâce à des tests de basculement simplifiés et automatisés.

Avec le pack de reprise après sinistre avancée, vous pouvez effectuer des tests programmés et automatisés pour n'importe quel serveur sur une base hebdomadaire ou mensuelle, ce qui vous donne l'assurance d'une reprise rapide et réussie.

- **La vérification des captures d'écran alimentée par l'IA** est utilisée pour vérifier que les charges de travail sont opérationnelles dans le nuage.
- **Un rapport consolidé est créé après chaque session de test** avec les détails des tests pour chaque charge de travail.

Create recovery server

General Cloud Firewall Rules

Server configuration

CPU and RAM
1 vCore, 4 GB RAM

The cost of running this server is 1 compute point per hour.

Type: Warm Cold

Retention (last recovery point)
- 1 +

Production network

Cloud network
192.168.244.0/24

DHCP: Provided by cloud site Custom

IP address in production network
192.168.244.100

Test network

External test IP address

IP address
192.168.244.56

Automated test failover

Schedule
Monthly

Screenshot timeout / Min
5

Save as default timeout

In automated test failover, the system takes a screenshot of the latest recovery point and validates if the operating system of the recovery server can be started. The process starts automatically at scheduled intervals.

Each automated test failover that is performed consumes compute points.

DR_Server_W2K3_SP2_x64

Fallover Edit Delete

Details Activities

Server details

Original server
vm-Win-2012-ABA12

Description
-

Type
Warm

Status
OK

State
Standby

Last recovery point
Ready

Actual RPO
Compliant

Automated test failover

Schedule: Monthly
Screenshot timeout: 5 min
Last start: Jul 9, 2022 12:00 AM + 02:00
Last status: Success
Next start: Jul 10, 2022

Show screenshot

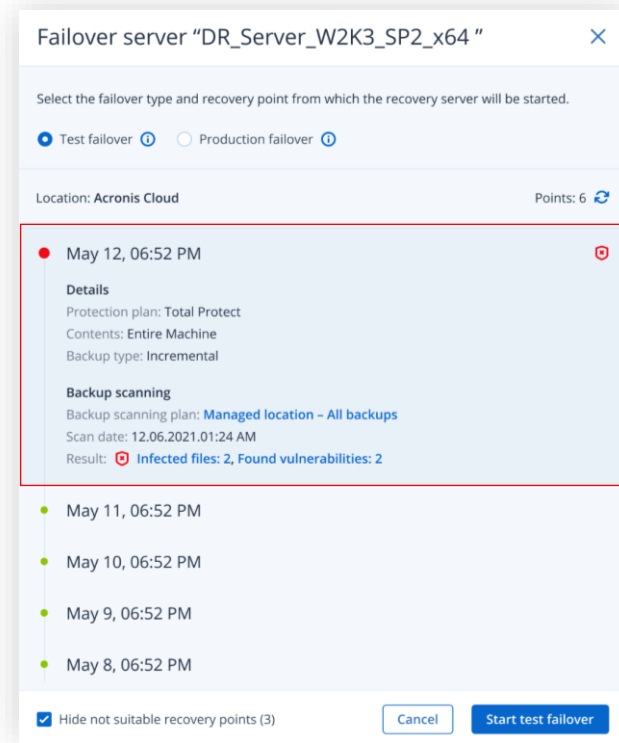
Basculement vers un point de récupération exempt de logiciels malveillants

Éviter la réinfection en étant proactif

Vérifier la liste des points de récupération disponibles pour les basculements **afin de voir si un logiciel malveillant ou un autre indicateur de compromission a été découvert** au cours du processus d'analyse des sauvegardes*.

Garantir un retour plus rapide et plus sûr à la productivité en empêchant la réinfection via un point de récupération compromis.

* Pour effectuer une analyse anti-malware des sauvegardes, la sécurité avancée doit être activée.



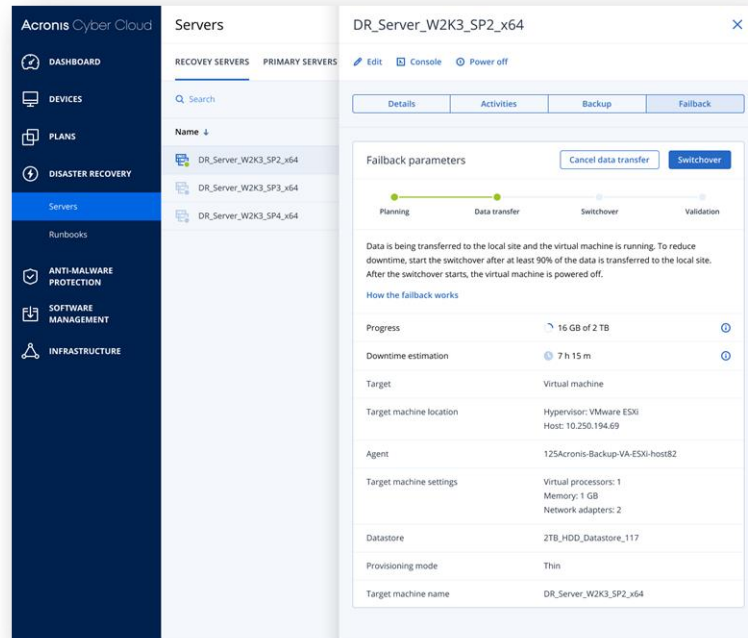
Why? Ensure successful recovery by selecting malware-free recovery points

Restauration automatique pour les machines physique et virtuelles (Fail back)

Réduction au maximum des interruptions d'activité

Procédez à une restauration automatique rapide et protégez les données de vos clients en les transférant sur le site local pendant que la machine virtuelle continue à s'exécuter dans le cloud. Vous êtes tenu au courant de l'état d'avancement du système et des interruptions d'activité prévues, de façon à planifier efficacement le processus de restauration automatique.

- Optimisez vos efforts en gérant l'ensemble du processus via une interface centralisée.
- Bénéficiez d'un des taux d'interruption d'activité les plus bas du marché pour le basculement.
- Éliminez toute confusion grâce à des instructions simples fournies via l'interface.



The screenshot displays the Acronis Cyber Cloud interface. On the left is a navigation sidebar with options: DASHBOARD, DEVICES, PLANS, DISASTER RECOVERY (highlighted), Servers, Runbooks, ANTI-MALWARE PROTECTION, SOFTWARE MANAGEMENT, and INFRASTRUCTURE. The main area is titled 'Servers' and shows a list of servers under 'RECOVERY SERVERS'. The selected server is 'DR_Server_W2K3_SP2_x64'. A detailed view for this server is open, showing 'Failback parameters'. The parameters include: Progress (16 GB of 2 TB), Downtime estimation (7 h 15 m), Target (Virtual machine), Target machine location (Hypervisor: VMware ESXi, Host: 10.250.194.69), Agent (125Acronis-Backup-VA-ESXi-host82), Target machine settings (Virtual processors: 1, Memory: 1 GB, Network adapters: 2), Datastore (2TB_HDD_Datastore_117), Provisioning mode (Thin), and Target machine name (DR_Server_W2K3_SP2_x64). A progress bar at the top of the parameters section shows the stages: Planning, Data transfer, Switchover, and Validation. The 'Switchover' stage is currently active.

Pourquoi ?

Réduction au maximum des interruptions, continuité des activités et protection des données de vos clients

Plus qu'une simple solution de reprise d'activité après sinistre

Acronis Cyber Protect Cloud

- ✓ Tests de basculement
- ✓ Connexion VPN cloud uniquement
- ✓ Gestion de groupes de ressources
- ✓ Plans centralisés
- ✓ Bureau à distance
- ✓ Inventaire des matériels
- ✓ Protection active
- ✓ Contrôle des terminaux
- ✓ Sauvegarde de fichiers, d'images et d'applications
- ✓ Acronis Instant Restore
- ✓ Etc.



Advanced Disaster Recovery

- ✓ Basculements de production ou en test
- ✓ Tests de basculement automatisé aidé par l'IA
- ✓ Cloud seul avec option de déploiement sans VPN
- ✓ VPN ouvert site-à-site L2
- ✓ VPN multisite IPsec
- ✓ Large choix de modèles
- ✓ Runbooks
- ✓ Configuration DNS et DHCP personnalisée



Acronis

#CyberFit

Merci !

Q&R

Acronis Cyber Foundation

Program

Transformer des vies grâce à l'éducation

Unissons nos efforts pour créer de nouvelles connaissances en mettant la diversité de nos expériences et de nos points forts au service d'un avenir plus radieux.



Rejoignez-nous !

