Acronis

Cyber Backup as a Service

WHAT'S NEW

IN THE ACRONIS CYBER CLOUD 8.0 RELEASE

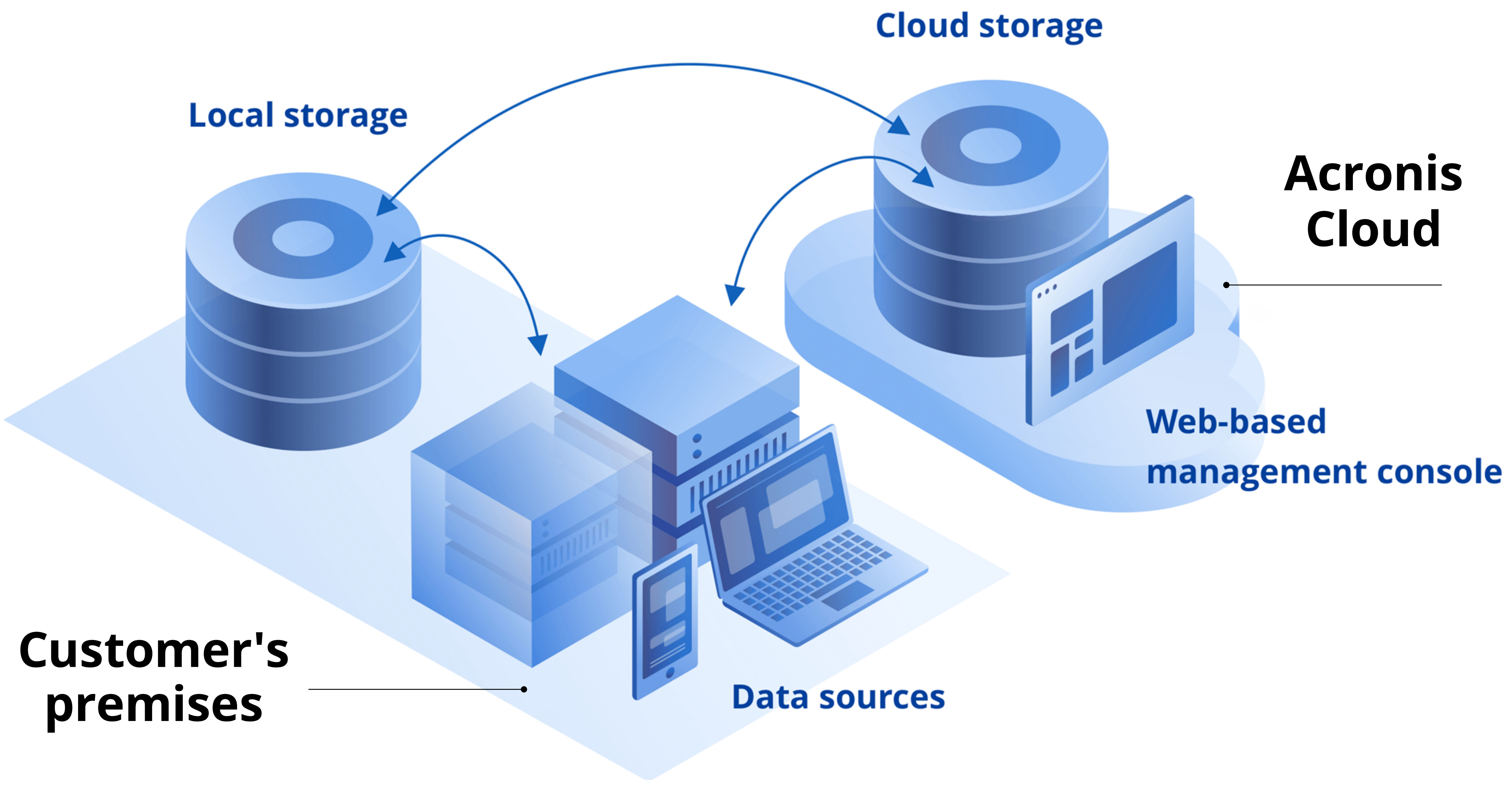
Acronis Cyber Backup as a Service

NOW FOR BOTH STANDARD AND ADVANCED EDITIONS

Acronis Cyber Backup is the best solution on the data protection market. It is available through two deployments models: on your premises or in the Acronis Cloud, without limiting functionally.

Acronis Cyber Backup as a Service leverages a wide variety of data protection capabilities including easy management of large environments, any-to-any recovery, cloud storage, cloud DR, and cloud-to-cloud backup of O365 and G Suite via a single, centralized web-based management console.

Get rid of on-premises backup complexity and explore the advanced functionality of Acronis Cyber Backup installed in the Acronis Cloud.



What's new in Acronis Cyber Backup as a Service

Easy

- Application-aware Hyper-V and Oracle Database backup and recovery
- Cluster-aware backup of Microsoft SQL Server and Microsoft Exchange Server
- Microsoft Office 365 public folders backup
- Granular Microsoft Exchange mailbox backup

Efficient

- New Performance and Backup window
- Centralized backup plan management and group management of devices
- Ability to add comments to devices
- Instant Restore with VM finalization for Hyper-V
- New device status rules
- Script-based backup location targeting

Secure

- Automatic backup file notarization
- Automatic system-information save, if a reboot recovery fails
- Encrypted backups support for disaster recovery
- Five locations for replication in a backup plan
- Secure Zone management from the backup console

...and new features in the **Acronis Disaster Recovery add-on**

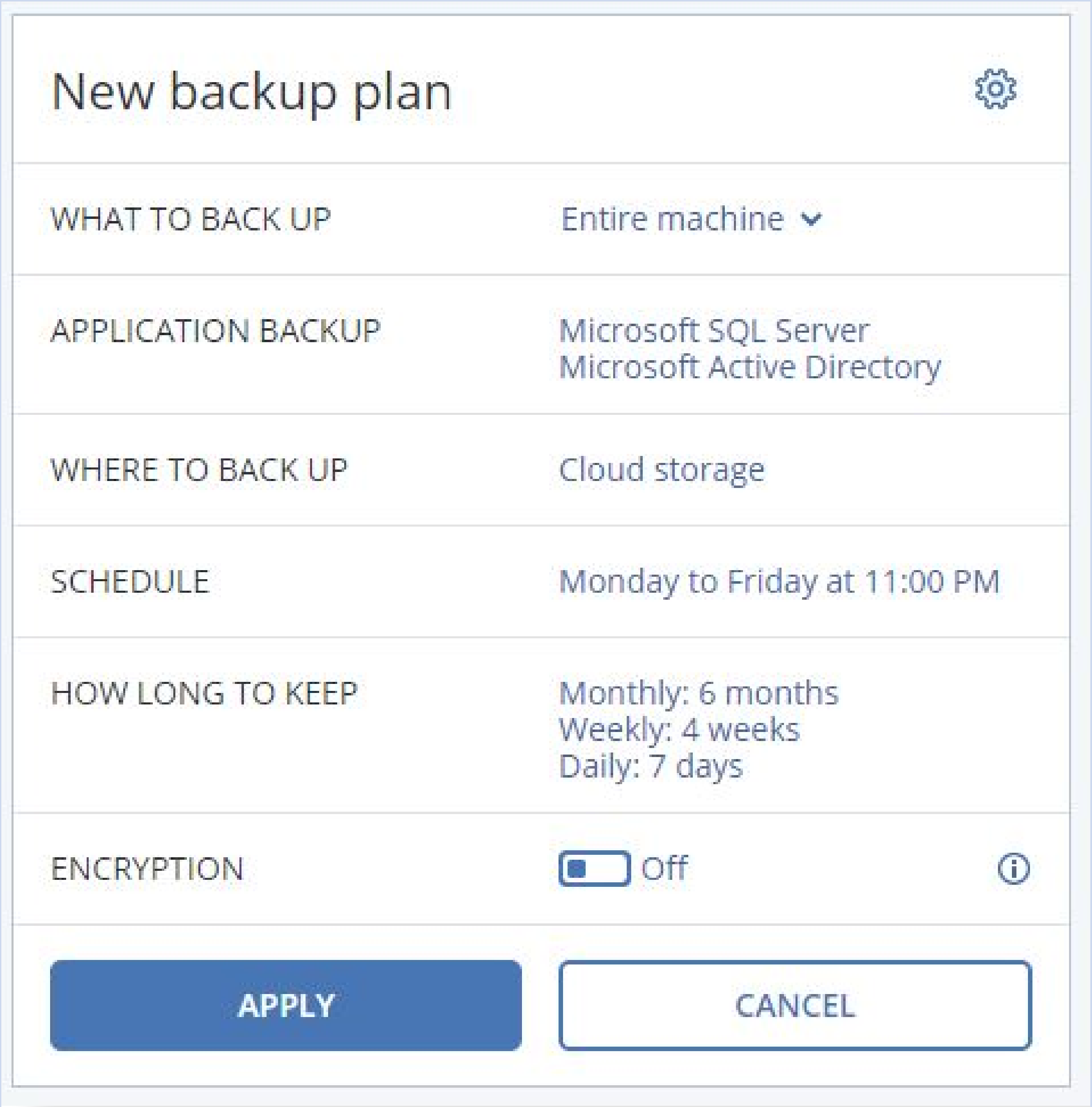
Easy

Application-aware VM backup on Hyper-V

Enable application-aware backup of Hyper-V VMs without the need to install per-VM agents

Gain ease-of-use and cost-efficiency.

The new application-aware backup of Hyper-V VMs by the Agent for Hyper-V improves backup and recovery of Microsoft SQL Server, Microsoft Exchange Server, Microsoft SharePoint, and Active Directory Domain Services running on Hyper-V.



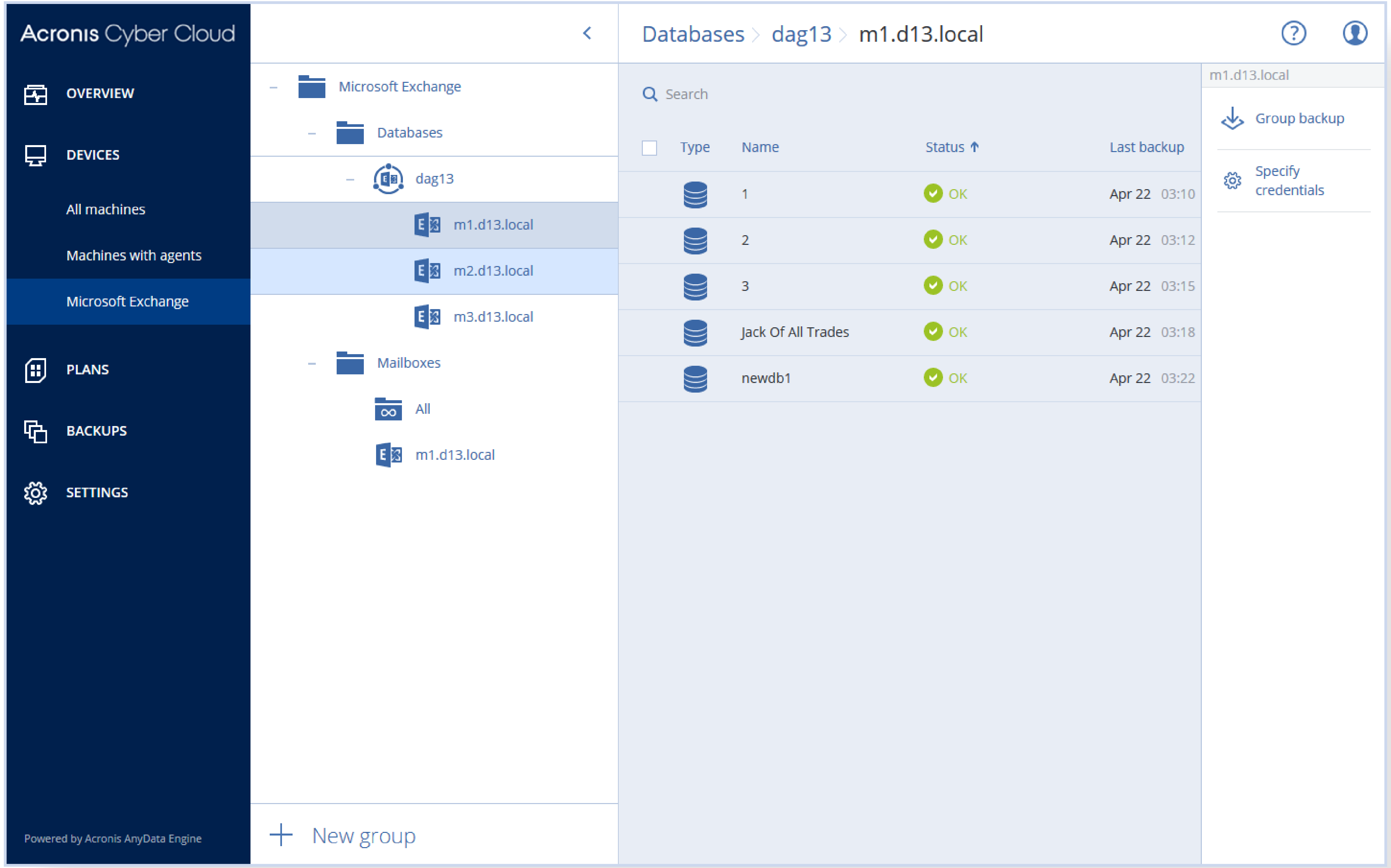
New backup plan

WHAT TO BACK UP	Entire machine
APPLICATION BACKUP	Microsoft SQL Server Microsoft Active Directory
WHERE TO BACK UP	Cloud storage
SCHEDULE	Monday to Friday at 11:00 PM
HOW LONG TO KEEP	Monthly: 6 months Weekly: 4 weeks Daily: 7 days
ENCRYPTION	Off

Cluster-aware backup of Microsoft SQL Server and Microsoft Exchange Server

Enable backup and reliable recovery of clustered Microsoft applications data, even in the event of a database logical corruption or a cluster-wide disaster.

Acronis Cyber Backup service discovers and takes into account the structure of the cluster and tracks all data relocation to enable safe backups.



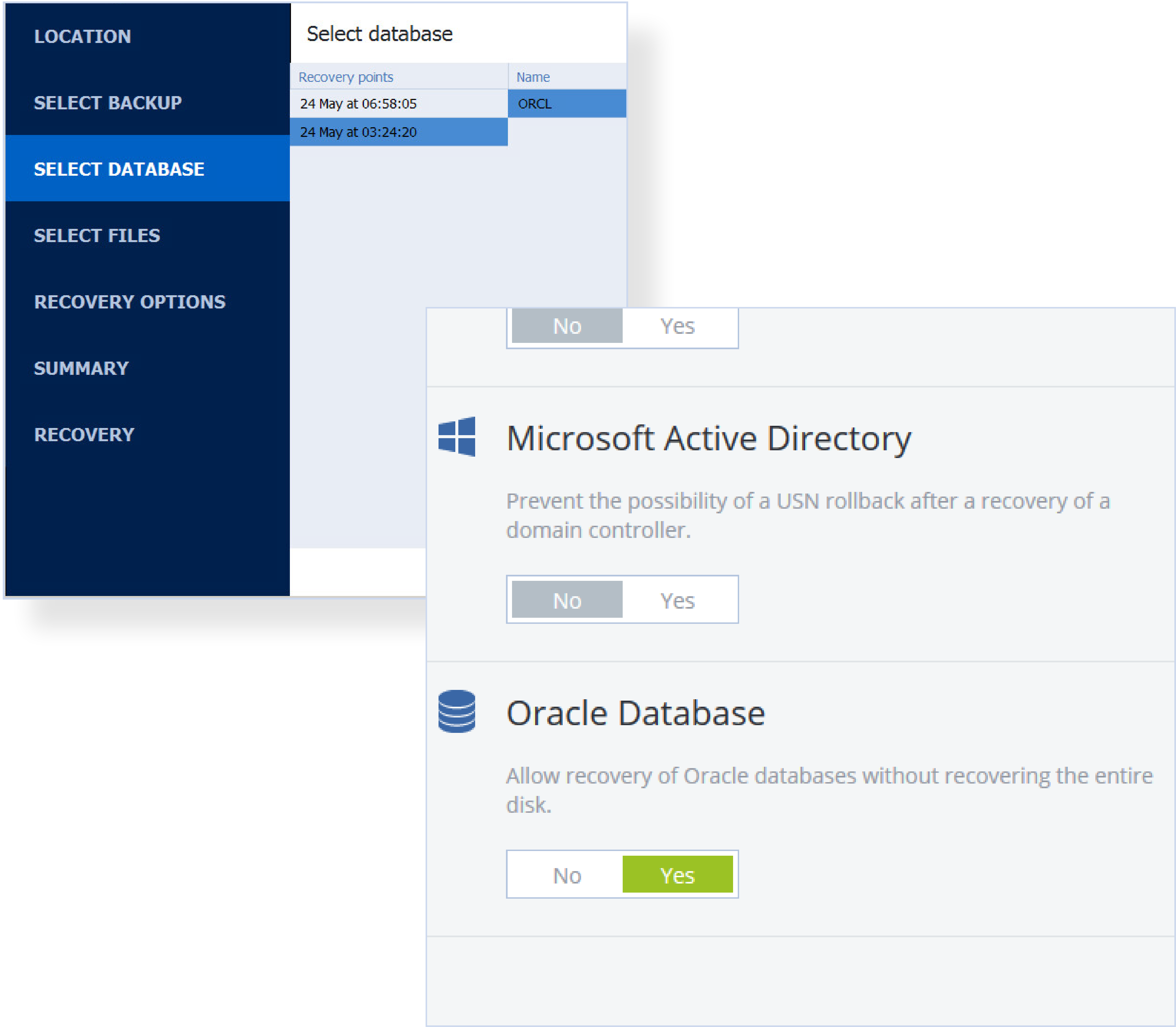
Type	Name	Status ↑	Last backup
	1	OK	Apr 22 03:10
	2	OK	Apr 22 03:12
	3	OK	Apr 22 03:15
	Jack Of All Trades	OK	Apr 22 03:18
	newdb1	OK	Apr 22 03:22

Application-aware Oracle Database backup

Protect Oracle Database data and ensure quick application recovery times

Acronis Cyber Backup as a Service now includes application-aware server-level and database-level backup and recovery for Oracle Database.

It also offers integration with RMAN for restoration and ready-to-use RMAN scripts for more sophisticated scenarios.



Select database

Recovery points	Name
24 May at 06:58:05	ORCL
24 May at 03:24:20	

[✓ No] Yes

Microsoft Active Directory

Prevent the possibility of a USN rollback after a recovery of a domain controller.

[✓ No] Yes

Oracle Database

Allow recovery of Oracle databases without recovering the entire disk.

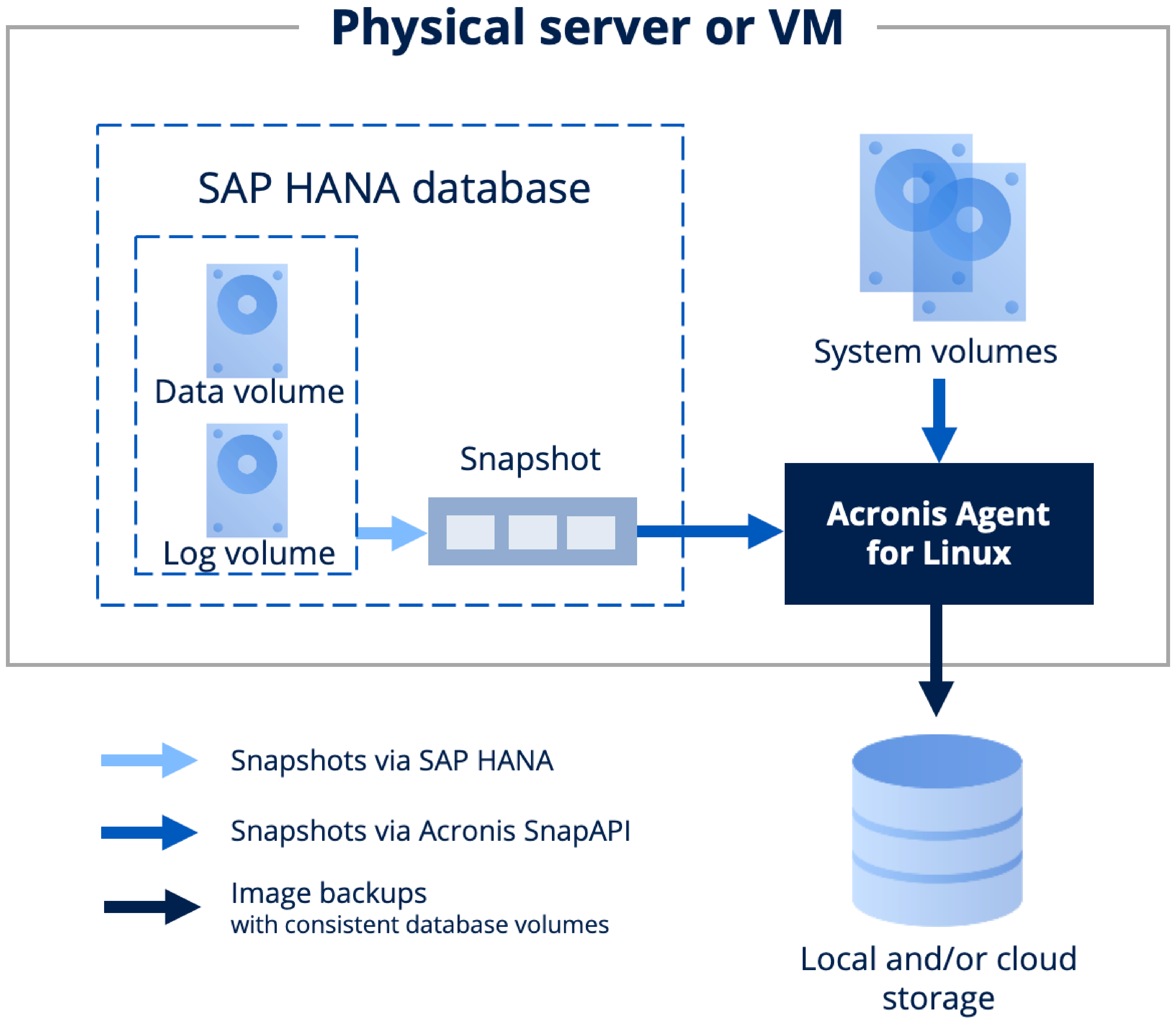
No [✓ Yes]

Application-aware SAP HANA backup

Enable quick, reliable recovery of SAP HANA database servers

To protect the database data from disk storage failures and logical errors, you can create consistent disk-level backups of servers running SAP HANA in a simple, straightforward manner that does not require any SAP HANA knowledge or expertise.

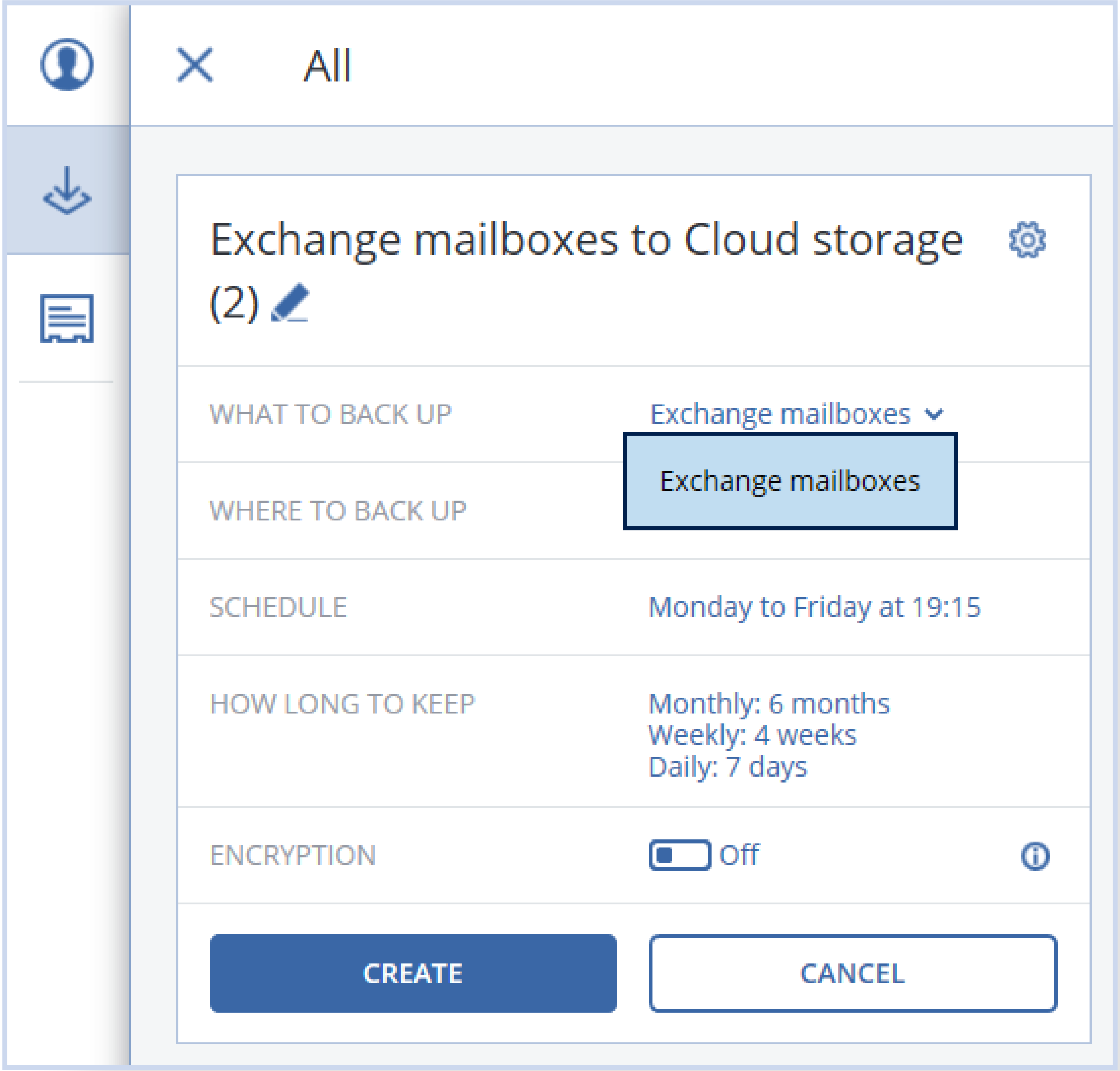
You can then reliably recover SAP HANA servers to bare metal, same or different hardware, and migrate them from a physical machine to a virtual machine and vice versa — the SAP HANA data inside the backup will be consistent.



Granular Microsoft Exchange mailbox backup

Back up and recover specific mailboxes without the need to back up the entire server or databases.

This backup is done remotely so there is no need to install the Exchange agent on the machine with the Exchange server.



All

Exchange mailboxes to Cloud storage (2)

WHAT TO BACK UP: Exchange mailboxes

Exchange mailboxes

WHERE TO BACK UP

SCHEDULE: Monday to Friday at 19:15

HOW LONG TO KEEP: Monthly: 6 months
Weekly: 4 weeks
Daily: 7 days

ENCRYPTION: Off

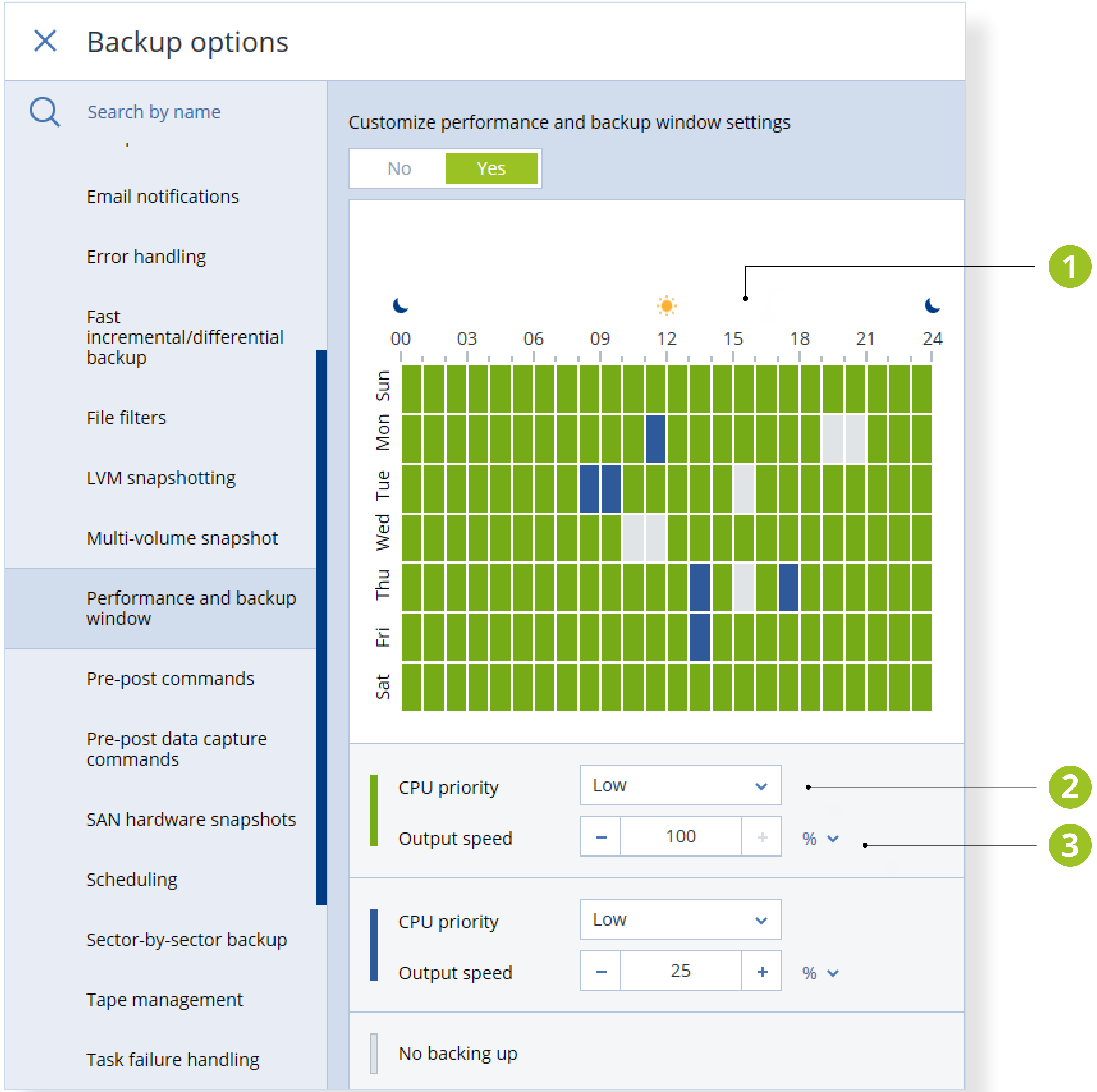
Efficient

Backup jobs time-window settings

Minimize the impact on running systems by setting backup window times in your backup plans

Set up backup window settings easily and minimize impact on running systems via the Performance and Backup window:

1. *Set up a preferred backup timeframe*
2. *Define the priority of the backup process in the operating system*
3. *Limit the output speed during backup process*



Backup options

Customize performance and backup window settings

No [✓ Yes]

Sun	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩
Mon	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟦	🟩	🟩	🟩	🟩	🟩	🟩	🟩	⬜	⬜	🟩	🟩	🟩
Tue	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟦	🟦	🟩	🟩	🟩	🟩	🟩	⬜	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩
Wed	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	⬜	⬜	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩
Thu	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟦	🟩	⬜	🟩	🟦	🟩	🟩	🟩	🟩	🟩	🟩
Fri	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟦	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩
Sat	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩

🟩 CPU priority: Low
Output speed: − 100 + %

🟦 CPU priority: Low
Output speed: − 25 + %

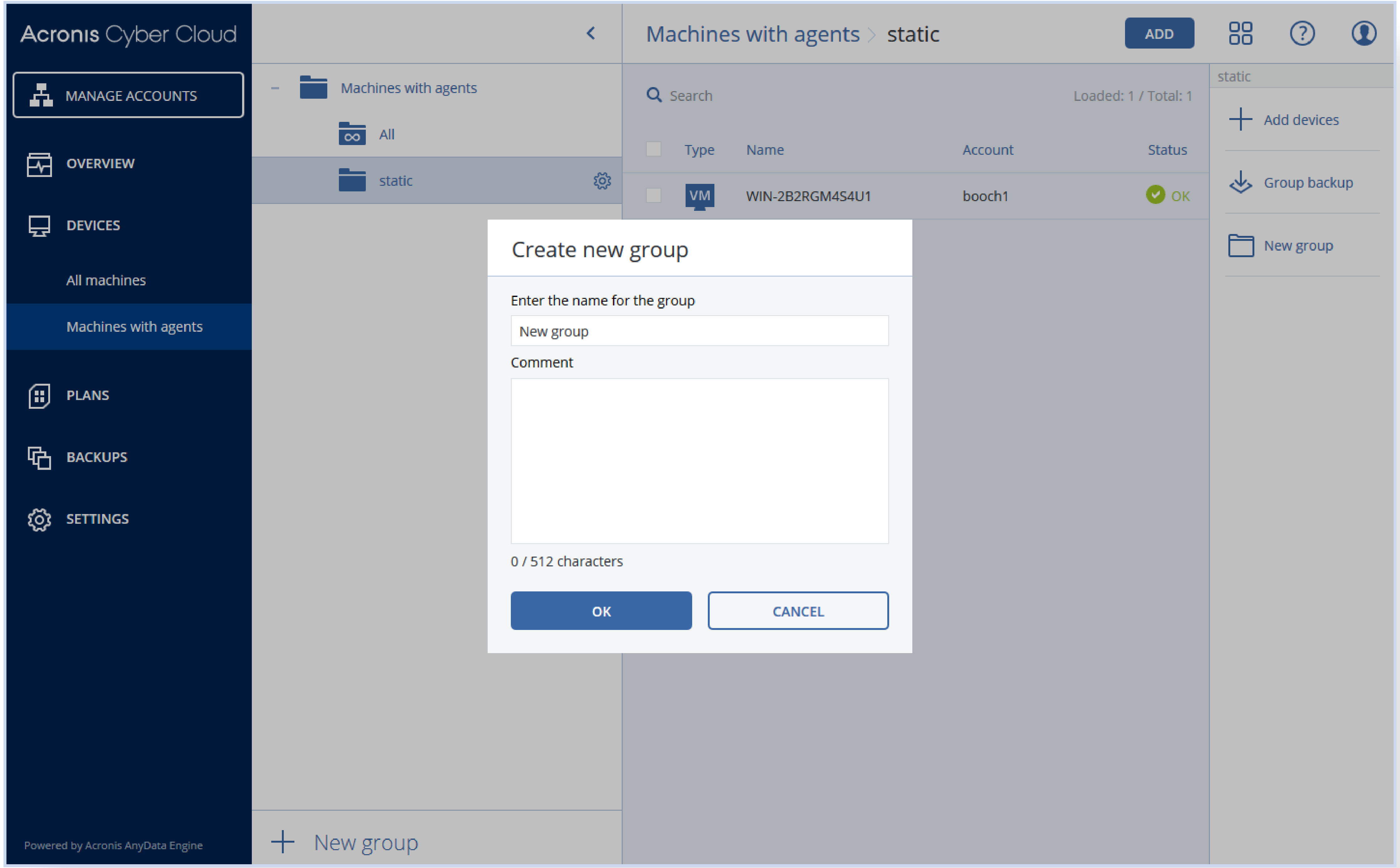
⬜ No backing up

Group management of devices

Manage a larger number of machines more quickly and easily

Create **static** or **dynamic** groups of machines and apply backup plans to the groups, not to each machine manually.

Once a new device is added to the group, the device automatically becomes protected by the specified backup plan.



Loaded: 1 / Total: 1

Type	Name	Account	Status
VM	WIN-2B2RGM4S4U1	booch1	OK

Create new group

Enter the name for the group: New group

Comment

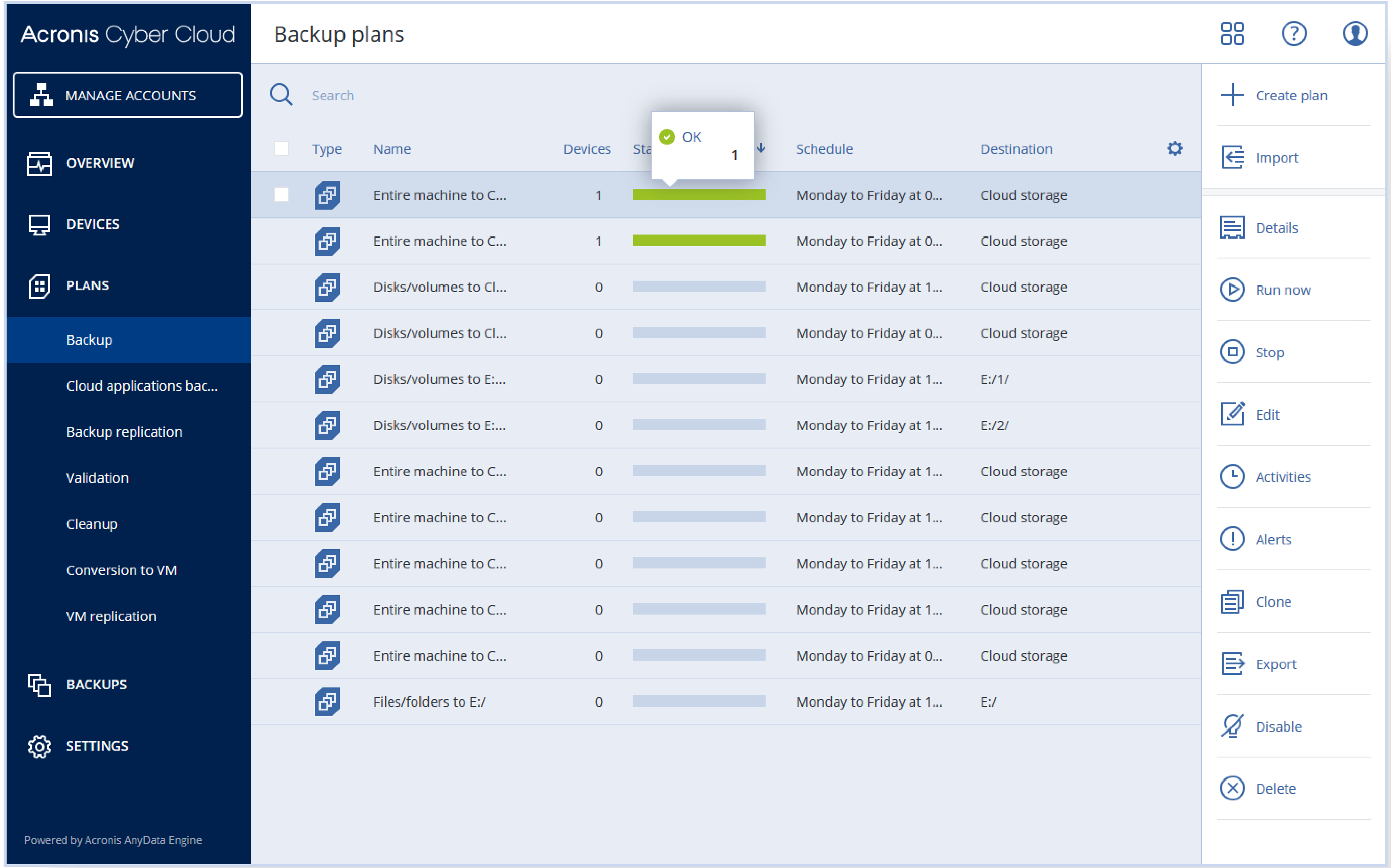
0 / 512 characters

Centralized backup plan management

Improve efficiency by managing backup plans from one tab

The new Plans tab shows all backup plans created in the account and their details.

You can create, edit, disable, enable, delete, start the execution of and inspect the execution status of a plan.



Backup plans

Type	Name	Devices	Sta	Schedule	Destination
	Entire machine to C...	1	🟩	Monday to Friday at 0...	Cloud storage
	Entire machine to C...	1	🟩	Monday to Friday at 0...	Cloud storage
	Disks/volumes to Cl...	0		Monday to Friday at 1...	Cloud storage
	Disks/volumes to Cl...	0		Monday to Friday at 0...	Cloud storage
	Disks/volumes to E:...	0		Monday to Friday at 1...	E:/1/
	Disks/volumes to E:...	0		Monday to Friday at 1...	E:/2/
	Entire machine to C...	0		Monday to Friday at 1...	Cloud storage
	Entire machine to C...	0		Monday to Friday at 1...	Cloud storage
	Entire machine to C...	0		Monday to Friday at 1...	Cloud storage
	Entire machine to C...	0		Monday to Friday at 1...	Cloud storage
	Entire machine to C...	0		Monday to Friday at 0...	Cloud storage
	Files/folders to E:/	0		Monday to Friday at 1...	E:/

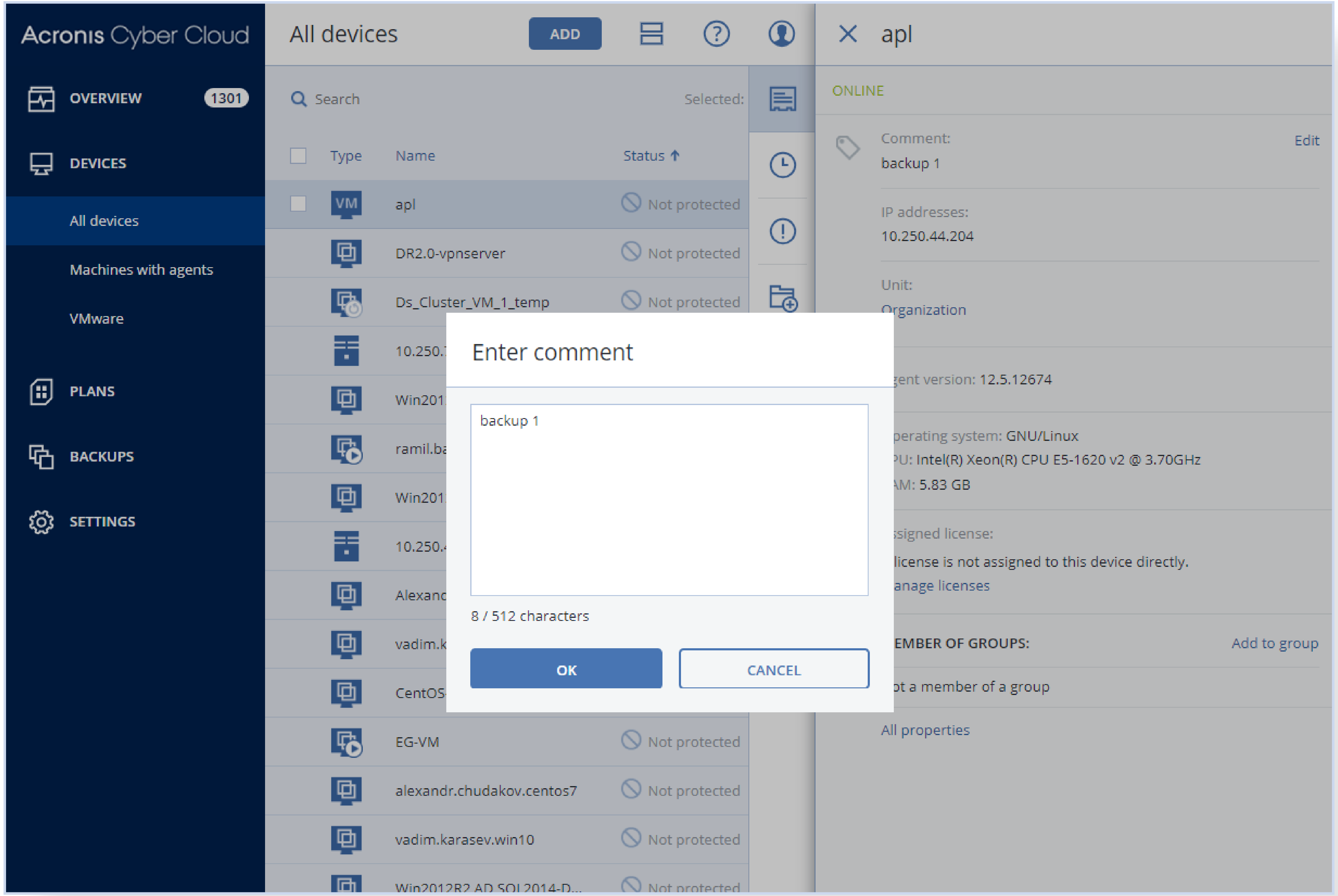
Ability to add comments to devices

Organize devices by adding comments to each protected machine on the Details pane then easily manage them by keywords

The new capability to Comment allows for convenient searches and device grouping among all protected systems.

By adding comments to your machines you can:

- Add useful notes for your team members
- Search for devices by keywords
- Group them by keywords **(Advanced edition)**



Type	Name	Status ↑
VM	apl	Not protected
	DR2.0-vpnserver	Not protected
	Ds_Cluster_VM_1_temp	Not protected
	10.250.	
	Win201	
	ramil.ba	
	Win201	
	10.250.	
	Alexand	
	vadim.k	
	CentOS	
	EG-VM	Not protected
	alexandr.chudakov.centos7	Not protected
	vadim.karasev.win10	Not protected
	Win2012R2 AD SQL2014-D...	Not protected

Enter comment

backup 1

8 / 512 characters

apl

ONLINE

Comment: backup 1

IP addresses: 10.250.44.204

Unit: Organization

gent version: 12.5.12674

perating system: GNU/Linux

U: Intel(R) Xeon(R) CPU E5-1620 v2 @ 3.70GHz

M: 5.83 GB

ssigned license:

license is not assigned to this device directly.

anage licenses

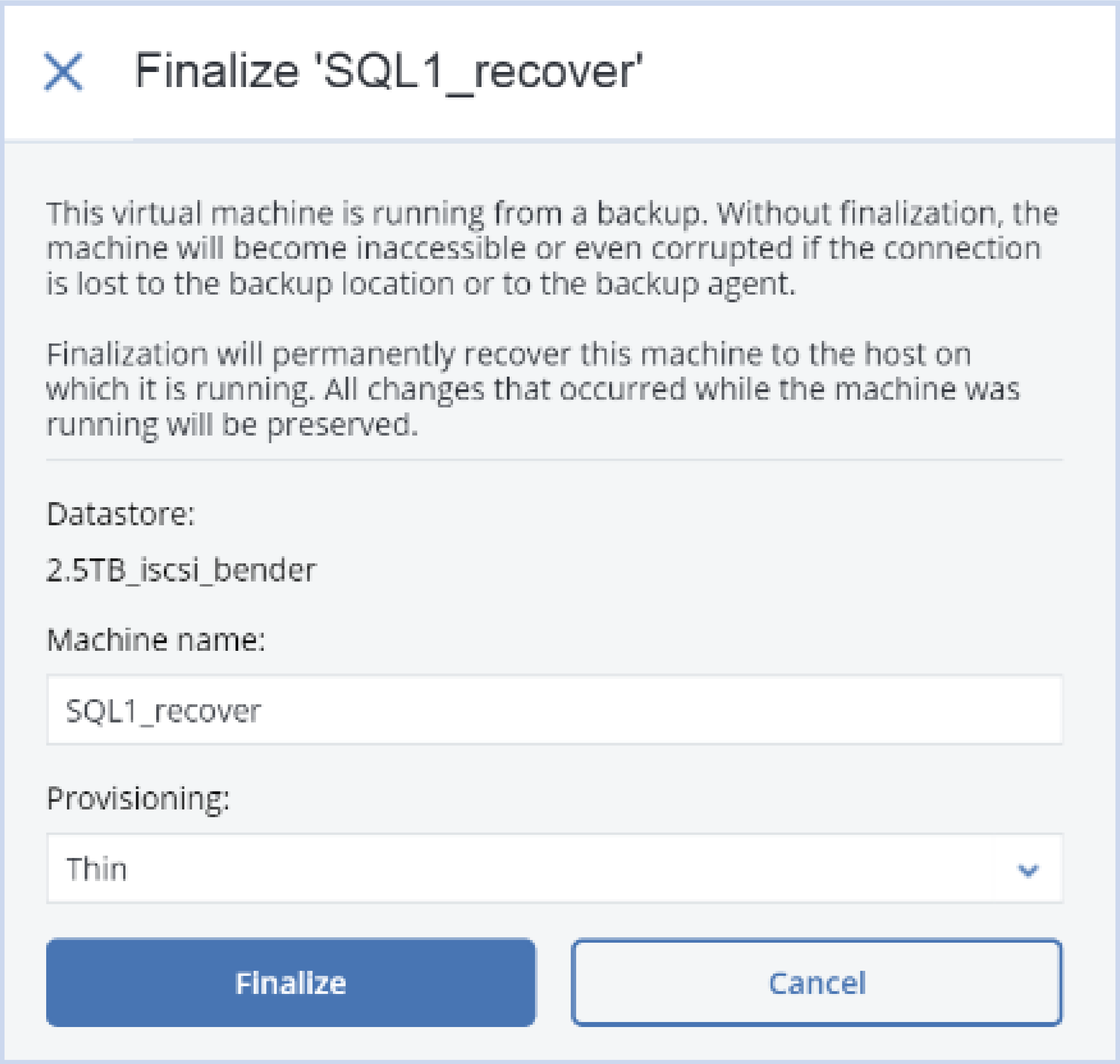
EMBER OF GROUPS:

ot a member of a group

VM finalization on Hyper-V

Finalize Hyper-V virtual machines that are running from backups during recovery via Acronis Instant Restore

Start Windows or Linux virtual machines immediately from backup storage. Get your virtual machine (VM) running in mere seconds while Acronis Instant Restore technology invisibly moves data in the background to the host — without any downtime.



Finalize 'SQL1_recover'

This virtual machine is running from a backup. Without finalization, the machine will become inaccessible or even corrupted if the connection is lost to the backup location or to the backup agent.

Finalization will permanently recover this machine to the host on which it is running. All changes that occurred while the machine was running will be preserved.

Datastore:
2.5TB_iscsi_bender

Machine name:
SQL1_recover

Provisioning:
Thin

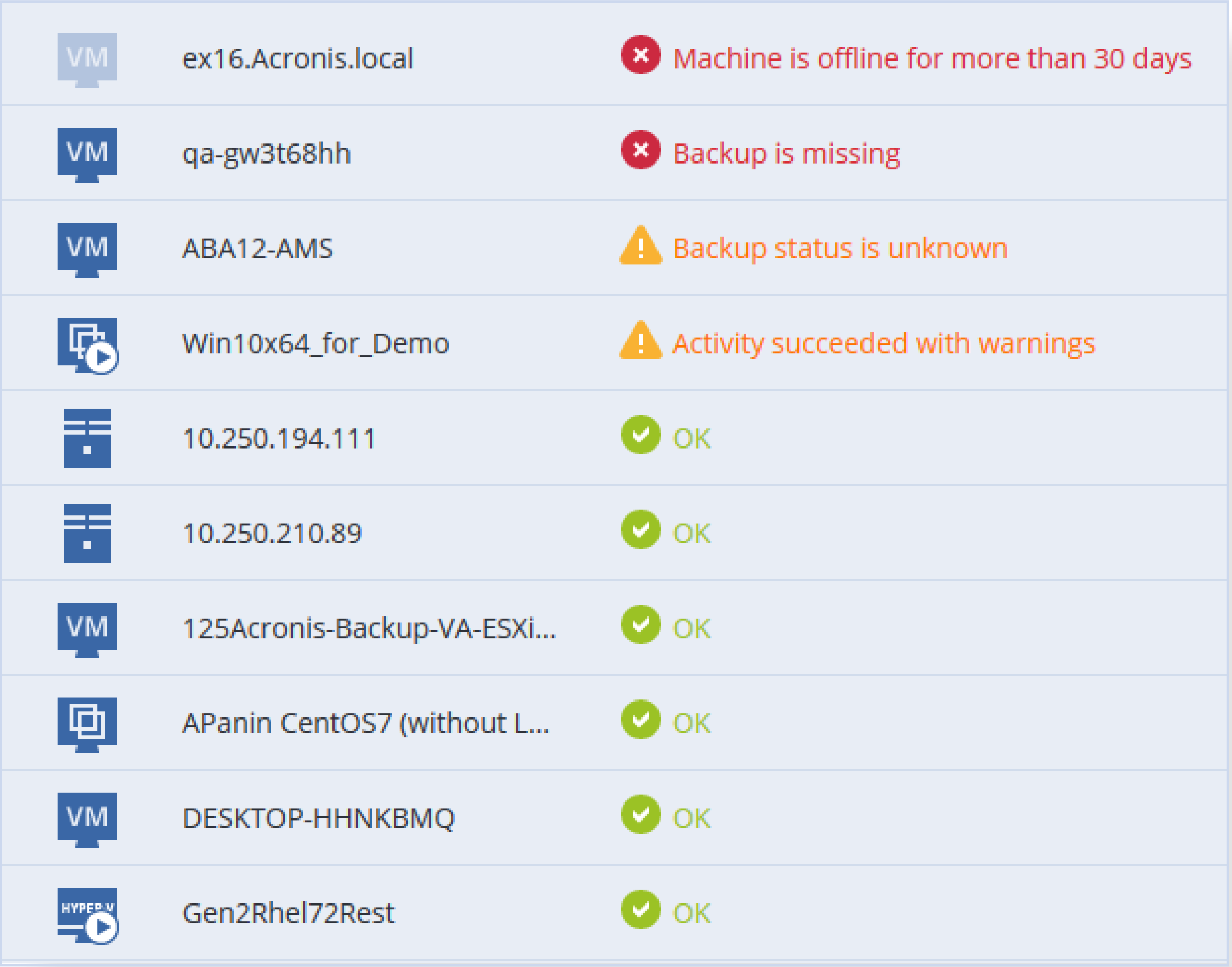
New device status rules

Troubleshoot faster with new alert-based statuses

Alerts cover a wider range of events than just backup activity results, e.g. missed backups and ransomware activities.

The statuses are now much more descriptive so you can quickly understand what the problem is (instead of just "error" or "warning" notices).

You can clear alerts manually — this will change the status to "OK".



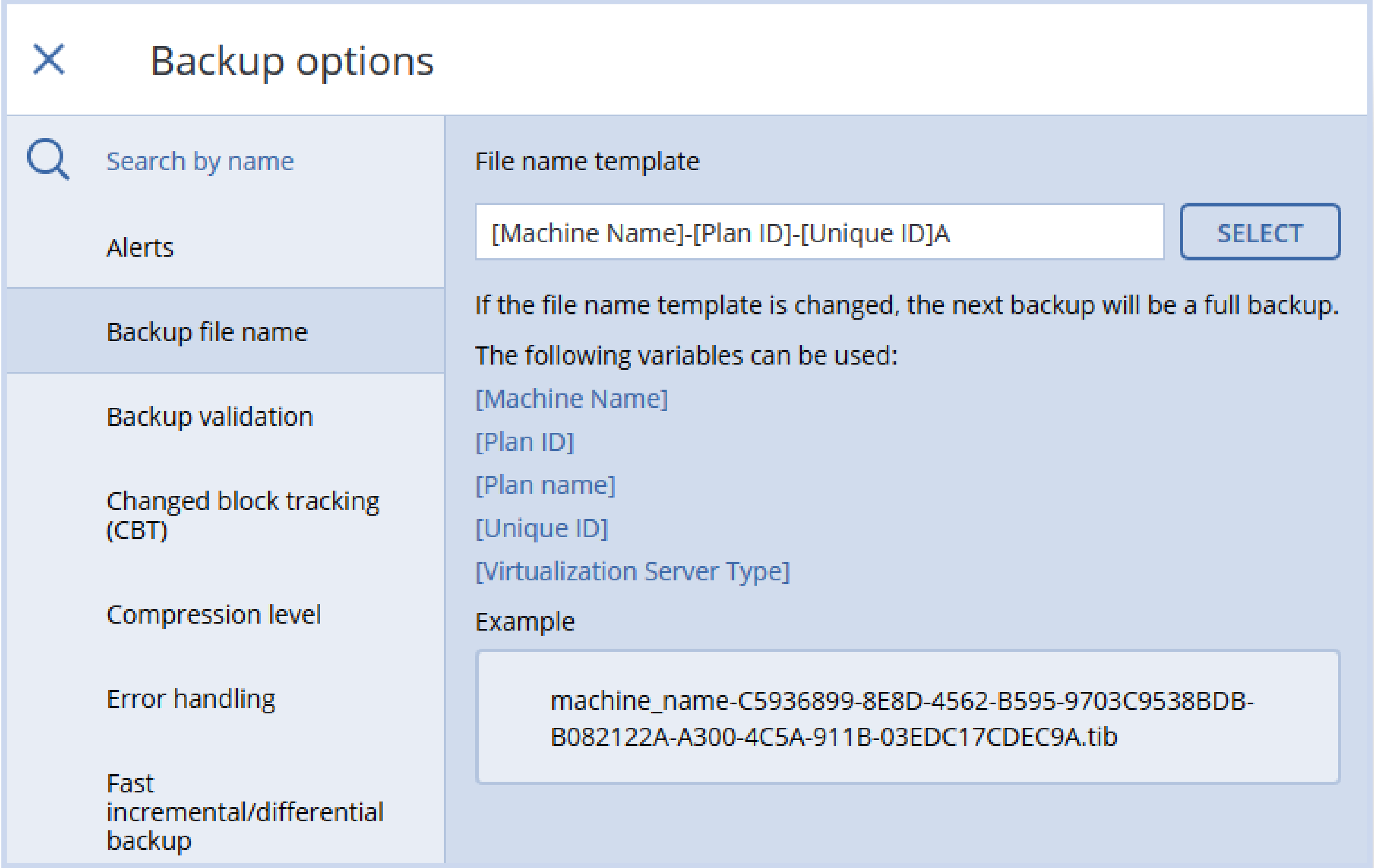
VM	ex16.Acronis.local	✖ Machine is offline for more than 30 days
VM	qa-gw3t68hh	✖ Backup is missing
VM	ABA12-AMS	⚠ Backup status is unknown
	Win10x64_for_Demo	⚠ Activity succeeded with warnings
	10.250.194.111	✓ OK
	10.250.210.89	✓ OK
VM	125Acronis-Backup-VA-ESXi...	✓ OK
	APanin CentOS7 (without L...	✓ OK
VM	DESKTOP-HHNKBMQ	✓ OK
HYPER-V	Gen2Rhel72Rest	✓ OK

New backup option: Backup file name

Continue an existing sequence of backups, no matter what

There are two main reasons to use the new backup file-name templates:

- To force the backup plan to continue backing up to the same backup or backup sequence — as opposed to starting a full backup from scratch.
- To benefit from more user-friendly backup file names, which you create manually.



Backup options

File name template

[Machine Name]-[Plan ID]-[Unique ID]A

If the file name template is changed, the next backup will be a full backup.

The following variables can be used:

[Machine Name]
[Plan ID]
[Plan name]
[Unique ID]
[Virtualization Server Type]

Example

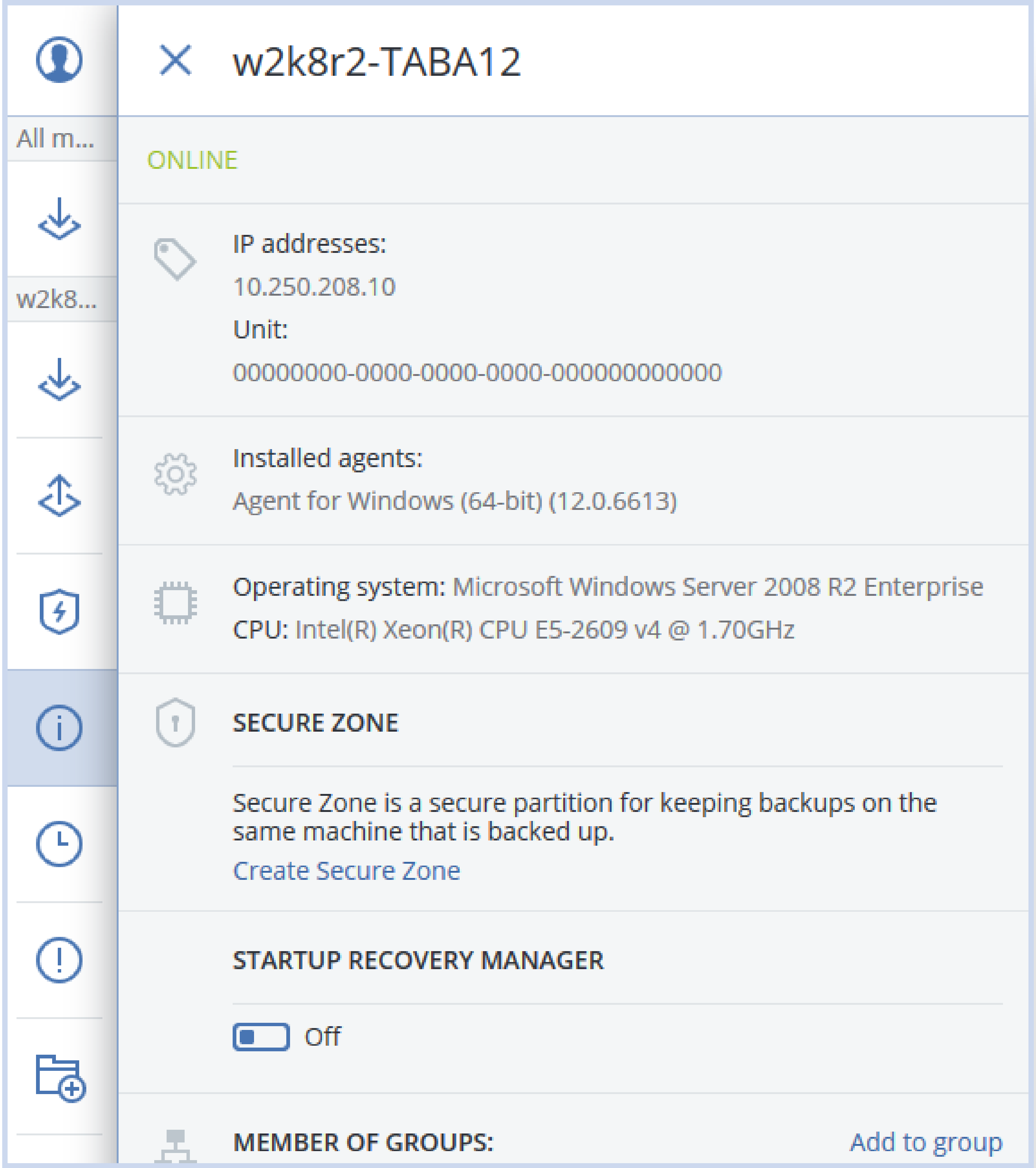
machine_name-C5936899-8E8D-4562-B595-9703C9538BDB-B082122A-A300-4C5A-911B-03EDC17CDEC9A.tib

Startup Recovery Manager

Restore machines quickly, even if the operating system does not load – without separate rescue media or network connection

Startup Recovery Manager is a bootable component that lives on the system disk in Windows, or on the /boot partition in Linux (where it is configured to start by pressing F11 at boot up).

On Windows and Linux machines, activate the Startup Recovery Manager using the backup console.



w2k8r2-TABA12

ONLINE

IP addresses:
10.250.208.10
Unit:
00000000-0000-0000-0000-000000000000

Installed agents:
Agent for Windows (64-bit) (12.0.6613)

Operating system: Microsoft Windows Server 2008 R2 Enterprise
CPU: Intel(R) Xeon(R) CPU E5-2609 v4 @ 1.70GHz

SECURE ZONE

Secure Zone is a secure partition for keeping backups on the same machine that is backed up.
Create Secure Zone

STARTUP RECOVERY MANAGER

Off

MEMBER OF GROUPS: Add to group

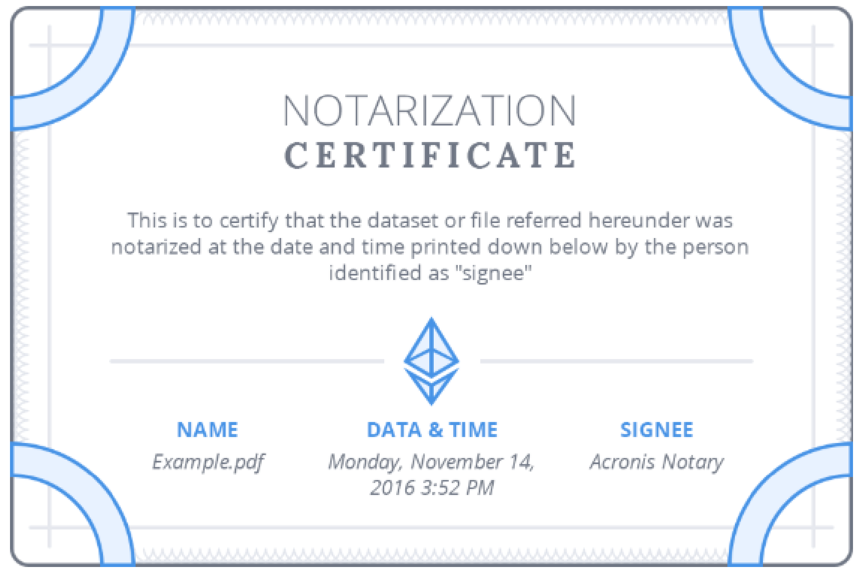
Secure

Backup file notarization option

Get independent validation that particular files are unchanged

To automatically notarize all files selected for backup, simply enable the Notarization option when you're creating a backup plan.

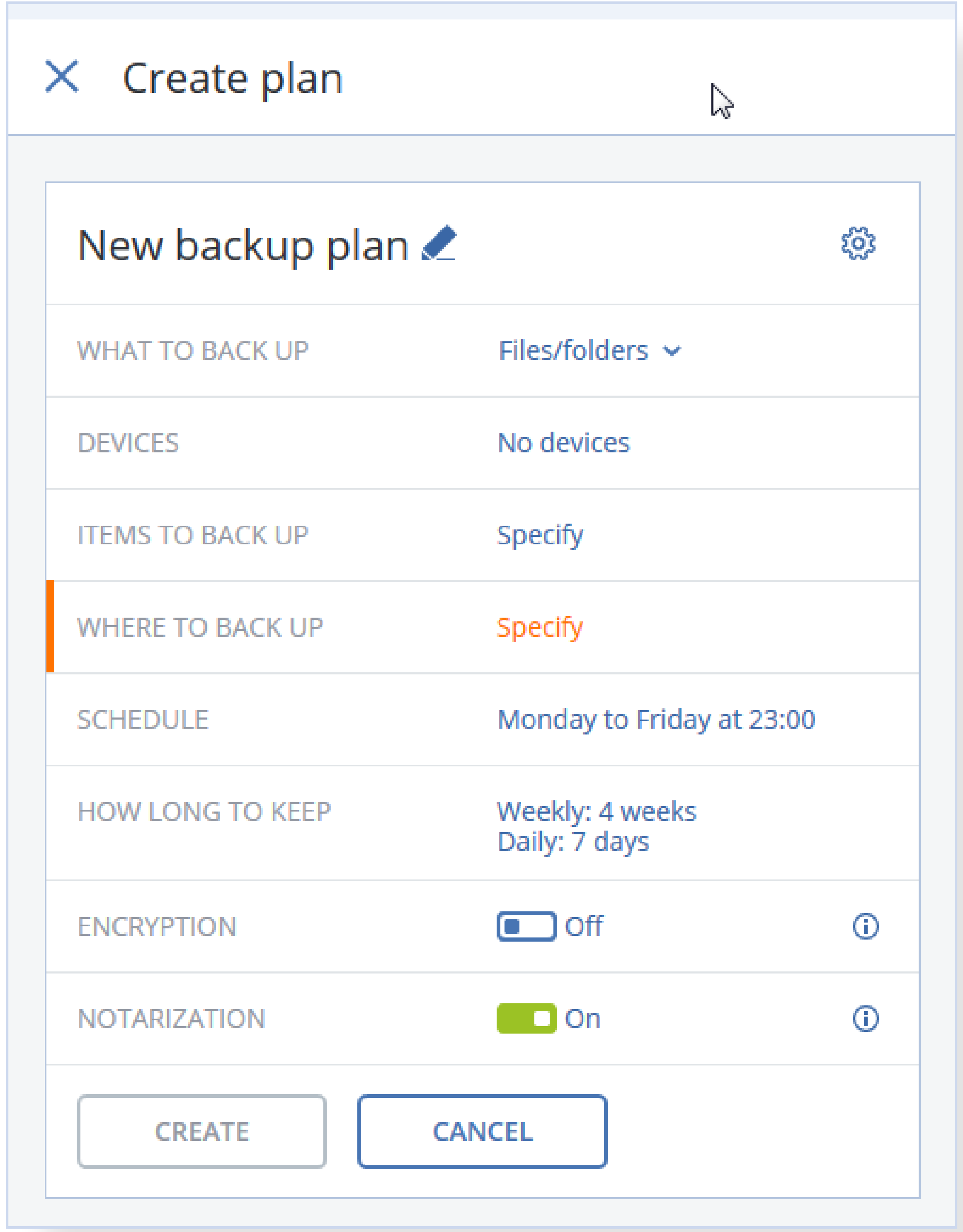
When configuring recovery, the notarized files will be marked with a special icon so you can easily verify the file's authenticity.



NOTARIZATION
CERTIFICATE

This is to certify that the dataset or file referred hereunder was notarized at the date and time printed down below by the person identified as "signee"

NAME	DATA & TIME	SIGNEE
Example.pdf	*Monday, November 14, 2016 3:52 PM*	*Acronis Notary*



Create plan

New backup plan

WHAT TO BACK UP	Files/folders
DEVICES	No devices
ITEMS TO BACK UP	Specify
WHERE TO BACK UP	Specify
SCHEDULE	Monday to Friday at 23:00
HOW LONG TO KEEP	Weekly: 4 weeks Daily: 7 days
ENCRYPTION	Off
NOTARIZATION	On

Easier Troubleshooting

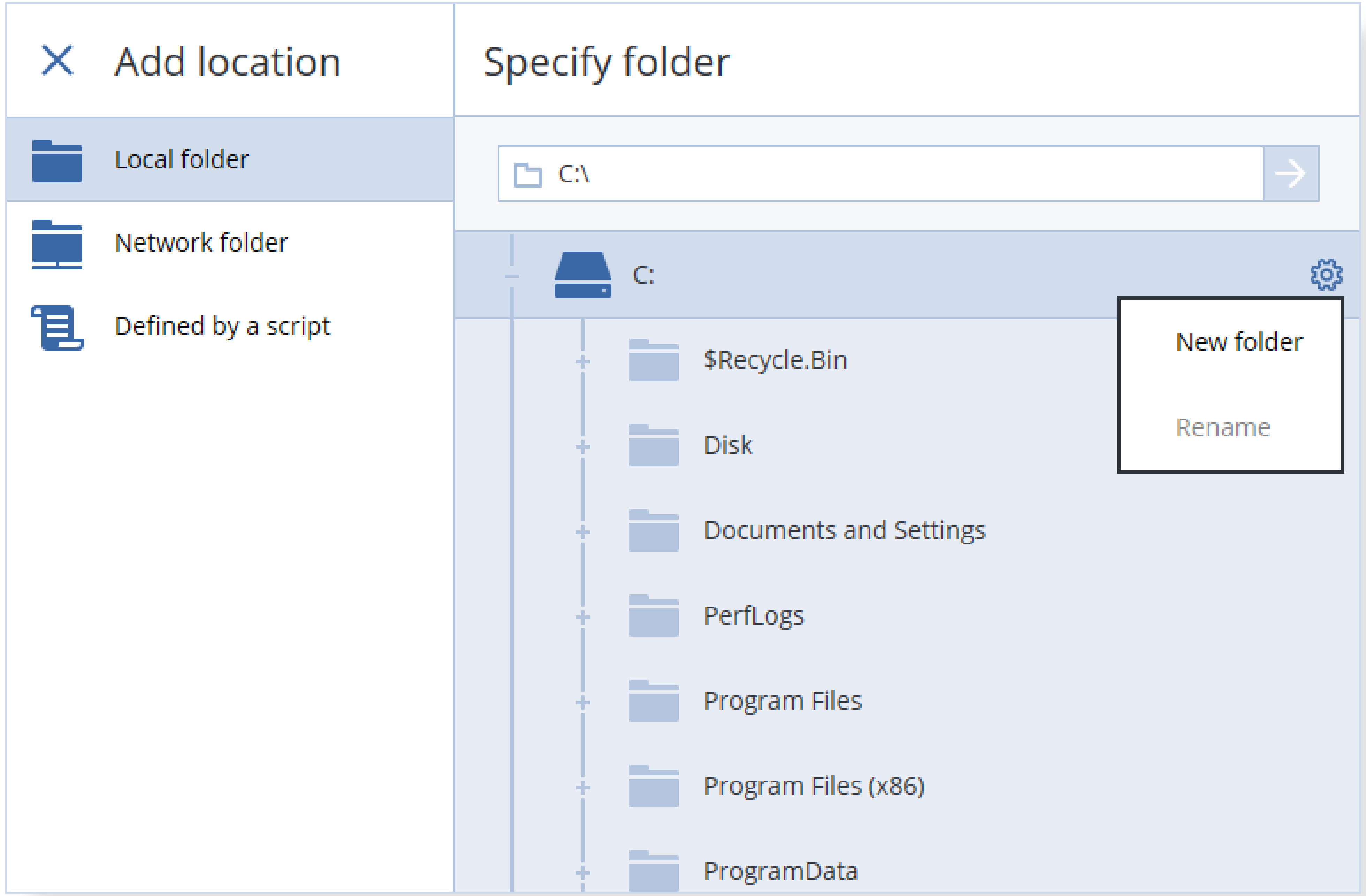
Streamline the work your IT staff needs to do to identify restore problems

Save system information on a local disk or a network share if a recovery with reboot fails. Specify a folder on the local disk or on a network share where the log, system information, and crash dump files will be saved.

Five locations for replication in a backup plan

Increase data safety and accessibility and balance data retention and storage costs more precisely

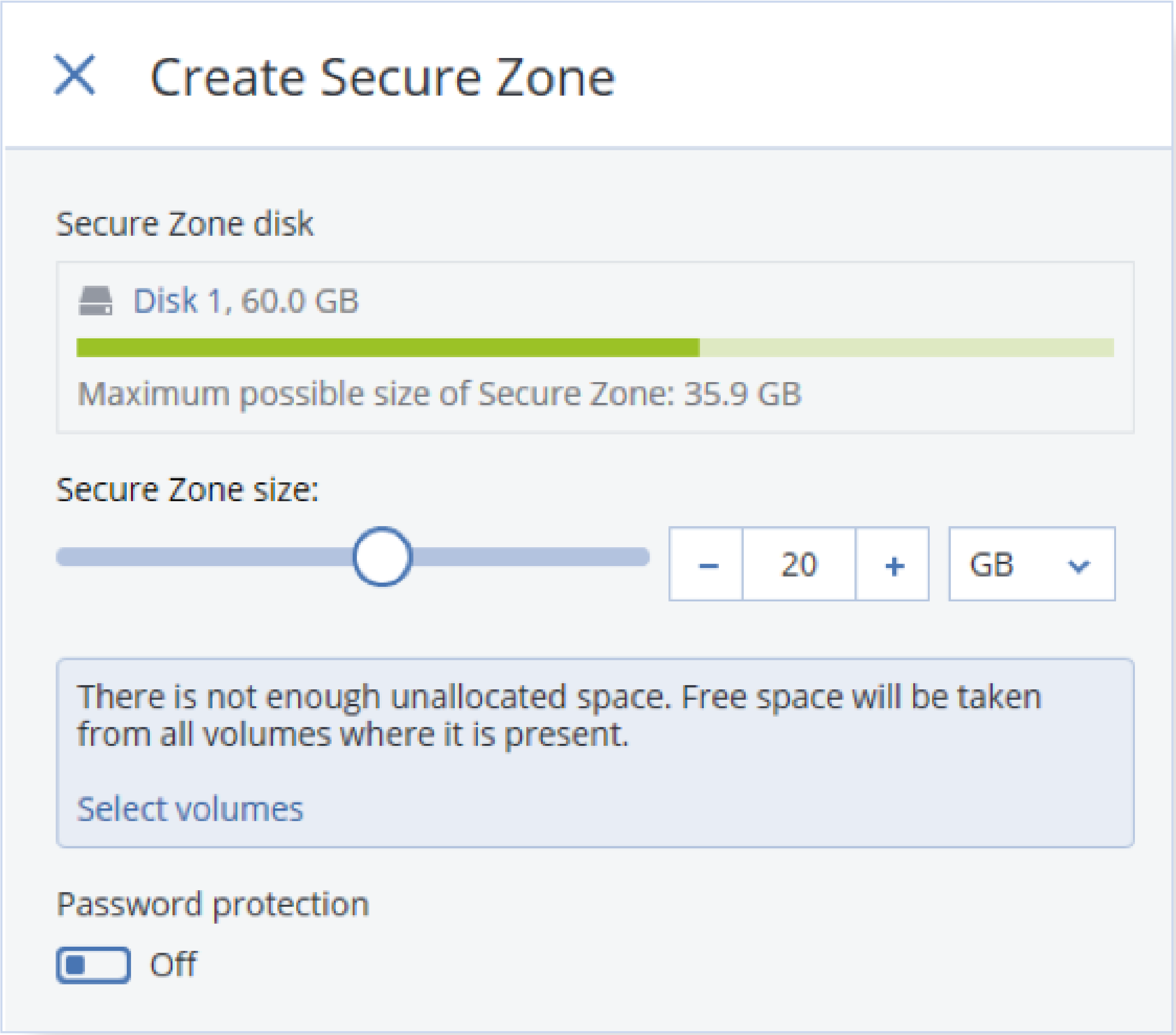
You can specify up to five locations where backups are replicated and set up separate rules for each location: retention rules, backup performance windows, and to-VM conversion settings.



Secure Zone management from the backup console

Create and delete Secure Zones on your protected machines without leaving the backup console. You can specify the Secure Zone size and enable password protection if needed.

Your Secure Zone is a secure partition on a disk of the backed-up machine, which is used to store the machine's backups. It is a useful, cost-effective method to protect backups from software malfunctions, virus attacks, or human error. It enables quick recovery from the same disk where the backup resides — with no need for a network connection or separate media to recover the data.



Create Secure Zone

Secure Zone disk

Disk 1, 60.0 GB

Maximum possible size of Secure Zone: 35.9 GB

Secure Zone size: 20 GB

There is not enough unallocated space. Free space will be taken from all volumes where it is present.

Select volumes

Password protection: Off

Other new features

Backup retention rule improvements

Specify how long to keep backups (e.g. based on the total size of backups in local storage) and when to start a cleanup procedure — before or after backups.

Assigning a virtual machine to a specific Agent for VMware (VM binding)

Assign a specific Agent for VMware to manage a specific virtual machine — as opposed to the default automatic agent-machine assignment. Manual binding is required in different cases, for example: if the Agent for VMware (virtual appliance) has locally attached storage, you will want to assign a dedicated agent to a very large VM; or, if you have multiple ESXi hosts that are separated geographically; etc.

Manual disk mapping when recovering machines

Re-map disks or volumes manually if you are dissatisfied with the disk-mapping result when performing recovery, or if the disk-mapping fails.

New recovery option: Boot mode

Select the boot mode that Windows will use after a recovery (BIOS or UEFI). If the original machine's boot mode is different from the selected boot mode, the software will initialize the recovery-to disk according to the option you select. Then it will adjust the Windows operating system so that it can start using the selected mode.

Default backup option management

Change a default option value against the pre-defined one for some backup options. The new value will be used by default in all backup plans created after you initiate the change.

Microsoft Office 365 public folder backup

Configure backup and recovery of Office 365 public folder data — in addition to many other types of items in Office 365.

New features in Acronis Disaster Recovery add-on

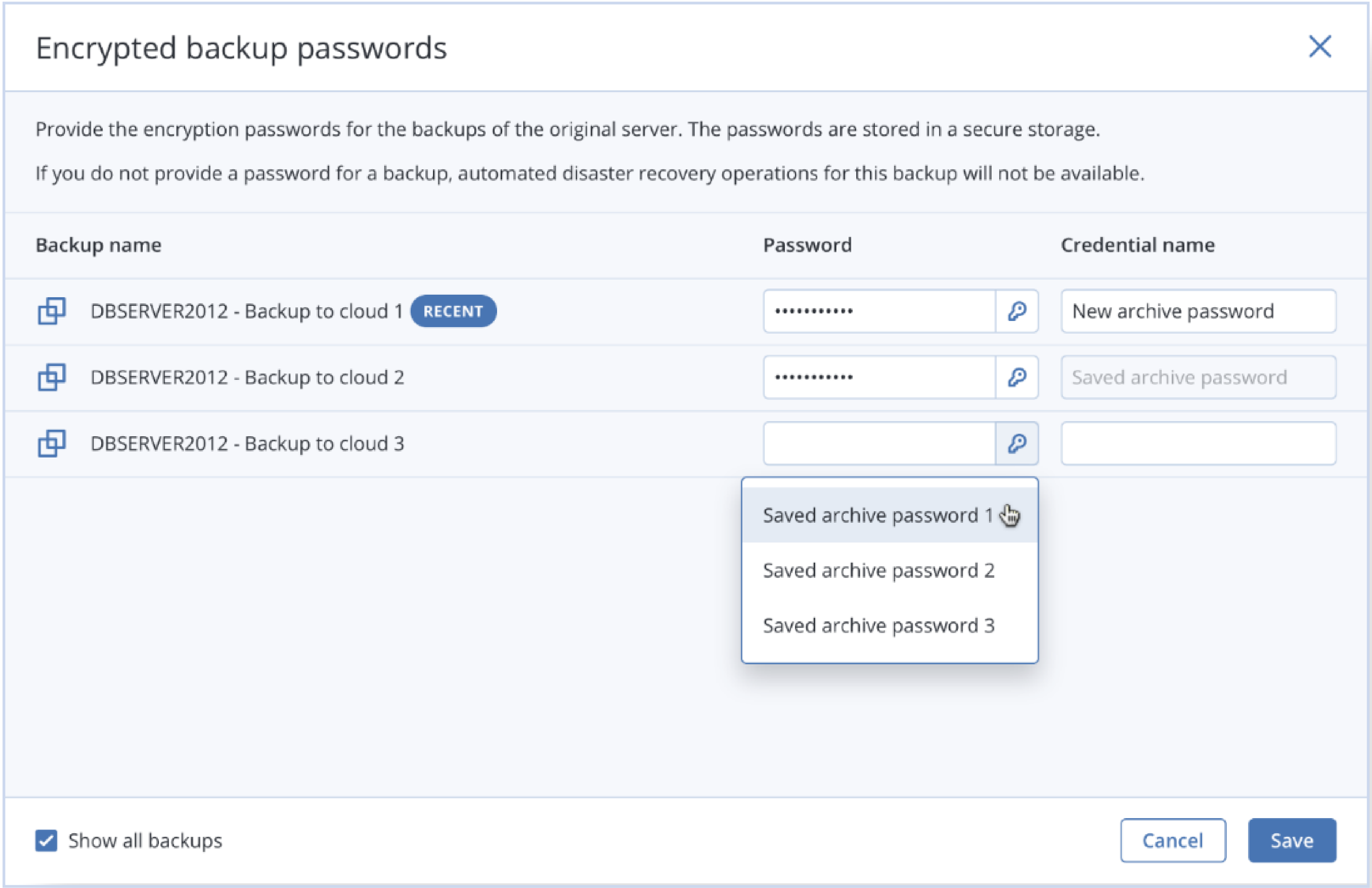
Encrypted backup support

Comply with data security requirements

Perform failovers using encrypted backups and allow the system to use securely stored passwords for automated disaster recovery operations.

The new Credential Store feature (accessible from the web console in the Disaster Recovery > Credential Store tab) allows you to securely store and manage passwords for encrypted server backups.

Comply with various data regulations (like HIPAA).



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.

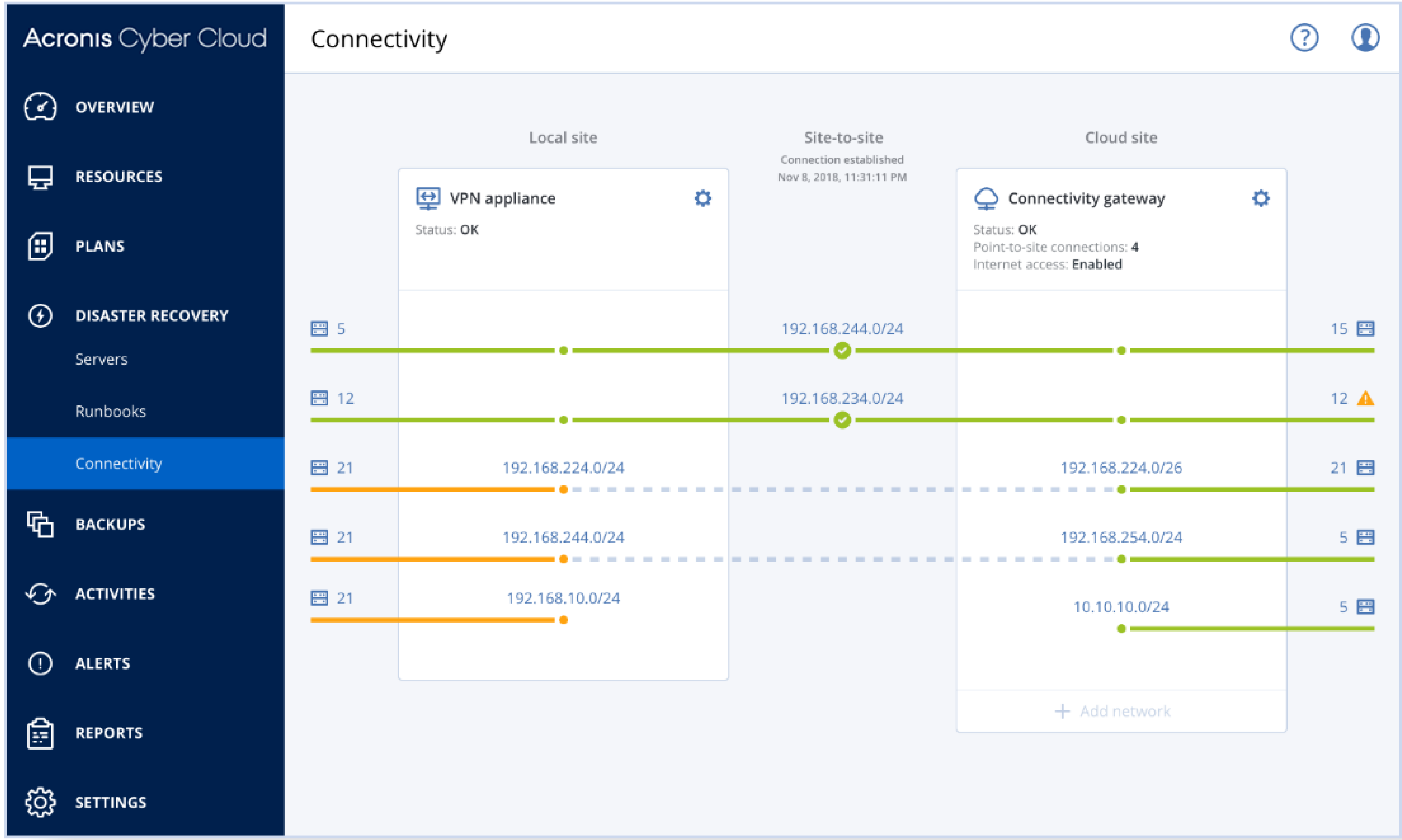
Backup name	Password	Credential name
DBSERVER2012 - Backup to cloud 1 RECENT	•••••••••••	New archive password
DBSERVER2012 - Backup to cloud 2	•••••••••••	Saved archive password
DBSERVER2012 - Backup to cloud 3		

☑ Show all backups

Multiple network support

Support more complex customer infrastructures

- Extend up to five local networks to the Acronis Cloud Recovery Site through the single site-to-site connection.
- Failover complex environments where protected servers are distributed across several network segments.
- See connectivity statuses of all five networks in one view.



Connectivity

Local site

VPN appliance
Status: OK

Site-to-site
Connection established
Nov 8, 2018, 11:31:11 PM

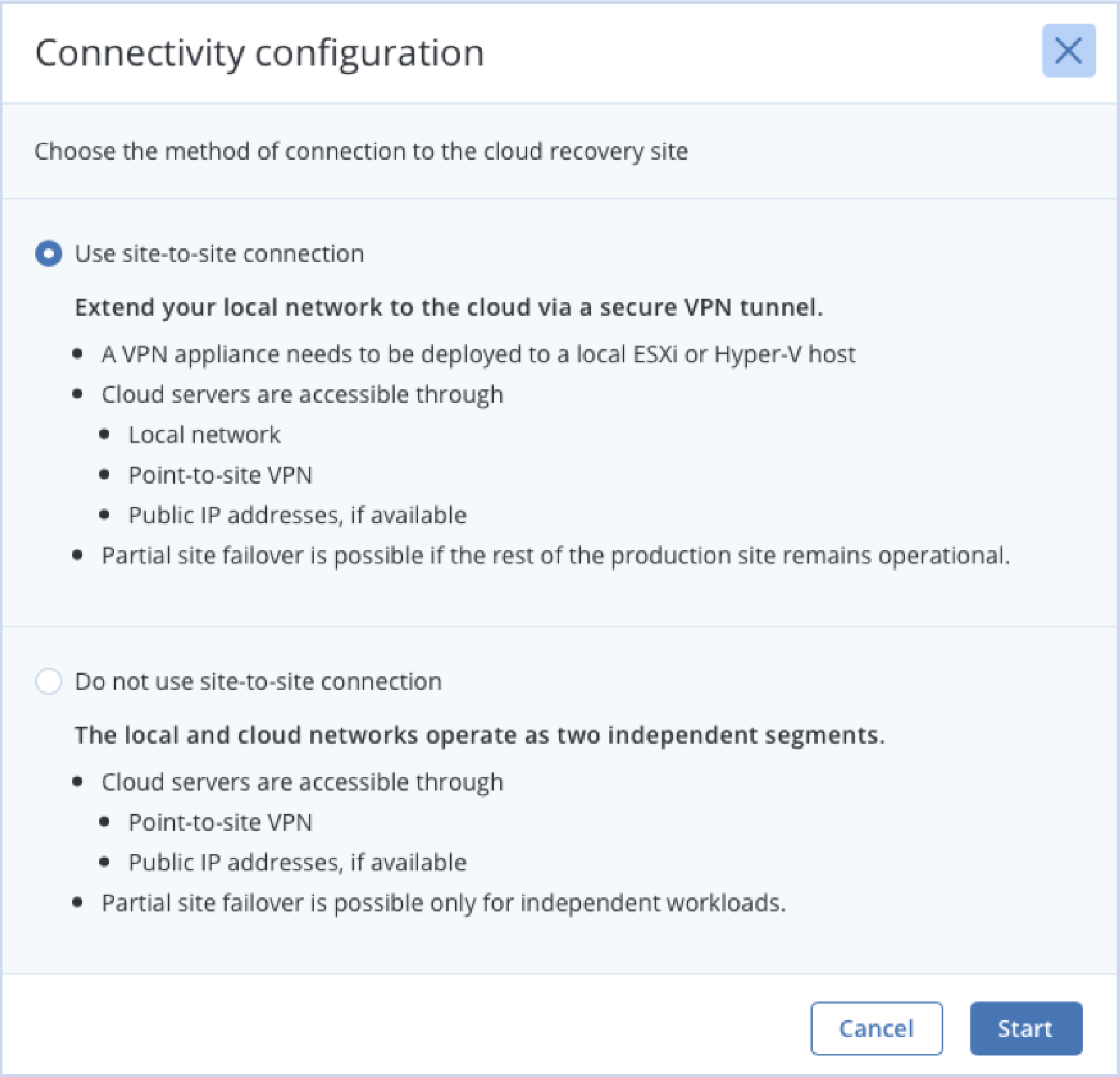
Cloud site

Connectivity gateway
Status: OK
Point-to-site connections: 4
Internet access: Enabled

VPN-less deployment option

Onboard customers more quickly and easily

- A VPN virtual appliance is not necessary for “point-to-site” connectivity.
- Switch from the “point-to-site” to “site-to-site” mode anytime.
- This option is especially useful for customers who want to quickly evaluate the service or don’t need to extend the local network to the cloud site.



Connectivity configuration

Choose the method of connection to the cloud recovery site

● Use site-to-site connection

Extend your local network to the cloud via a secure VPN tunnel.

- A VPN appliance needs to be deployed to a local ESXi or Hyper-V host
- Cloud servers are accessible through
  - Local network
  - Point-to-site VPN
  - Public IP addresses, if available
- Partial site failover is possible if the rest of the production site remains operational.

○ Do not use site-to-site connection

The local and cloud networks operate as two independent segments.

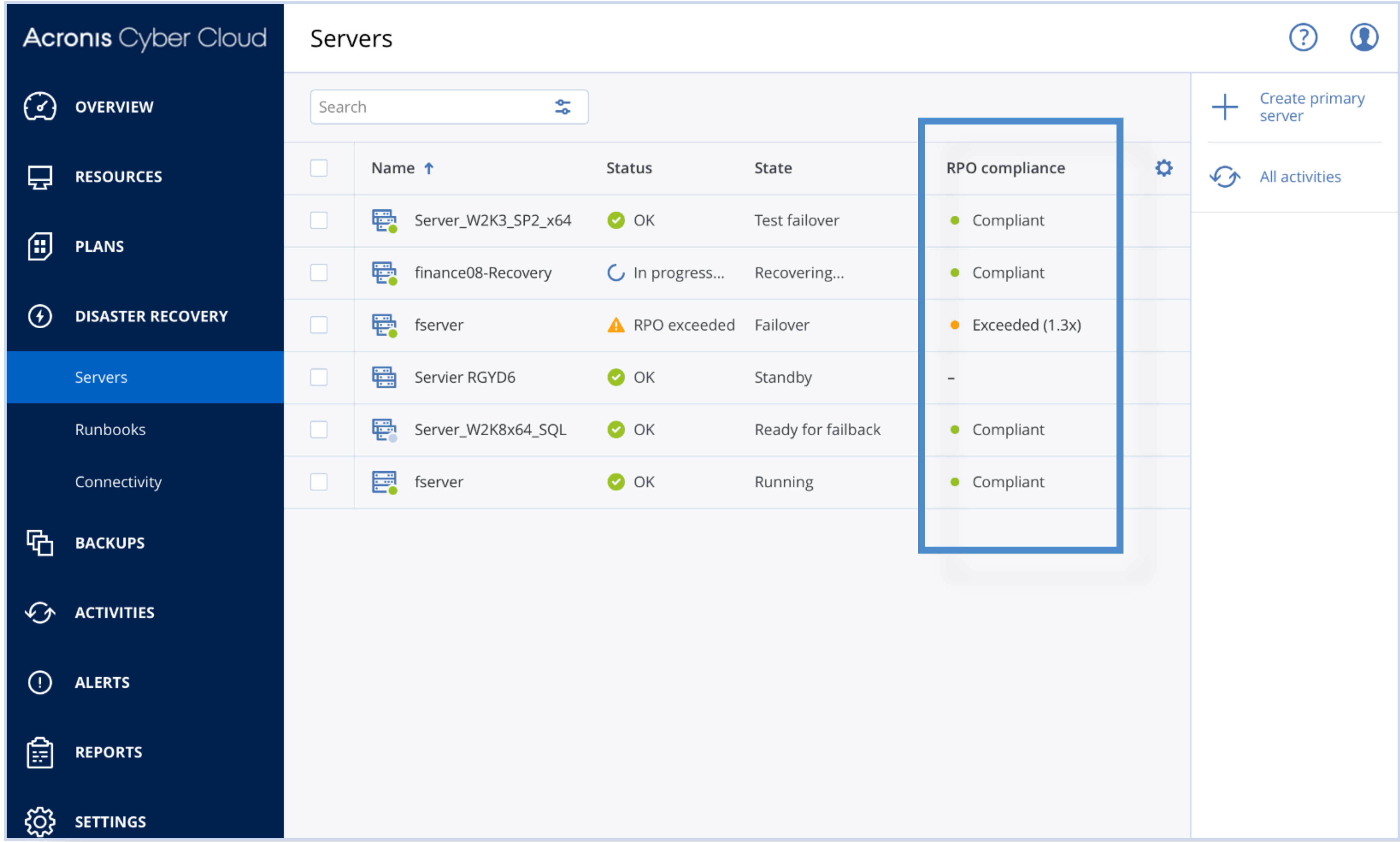
- Cloud servers are accessible through
  - Point-to-site VPN
  - Public IP addresses, if available
- Partial site failover is possible only for independent workloads.

Recovery servers RPO compliance tracking

Improve SLA compliance

Define recovery point thresholds for the recovery servers to identify how "fresh" the cloud backup of the original machine (to perform failover) should be.

Track recovery point objective (RPO) compliance in real-time via the web console. Get alerts if the threshold is exceeded.



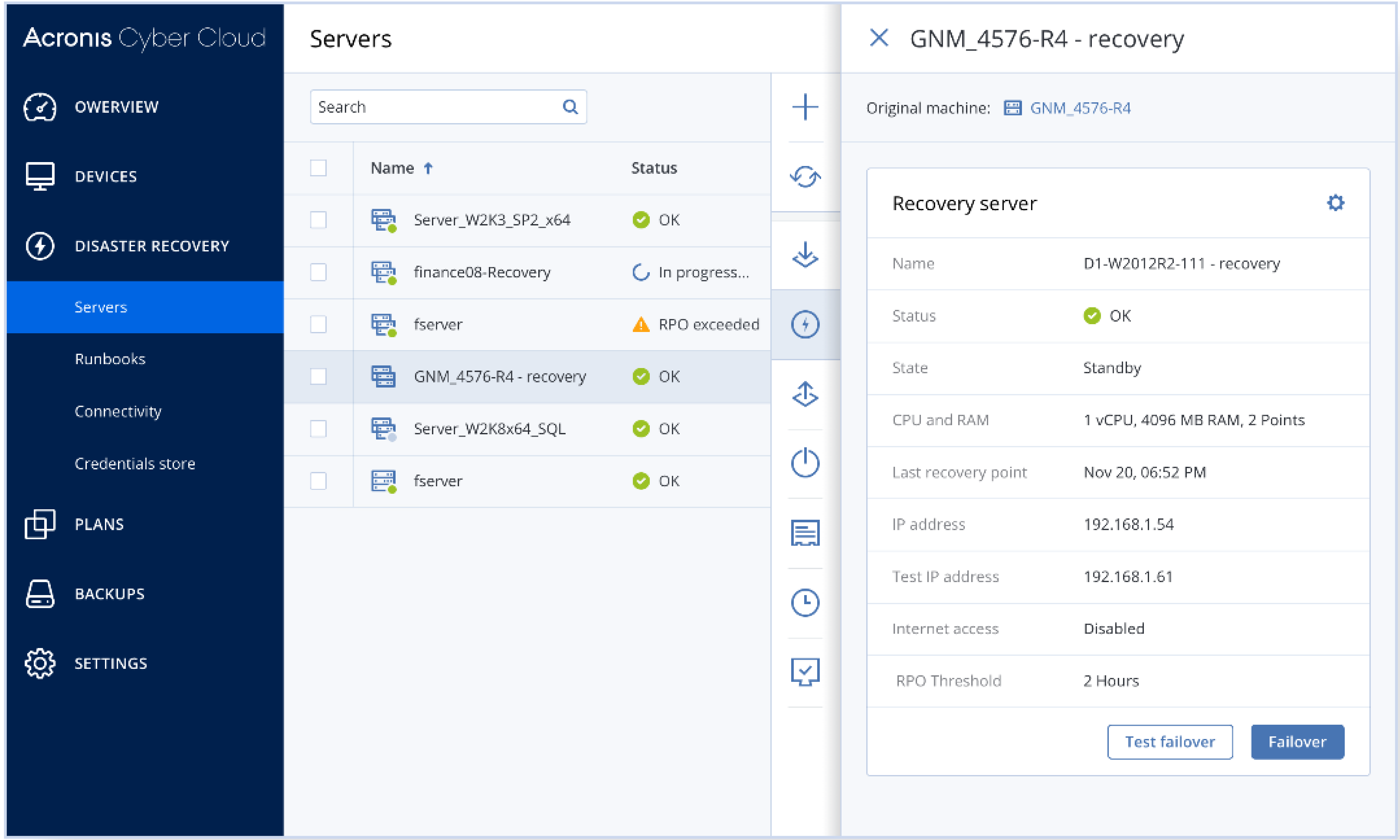
Name ↑	Status	State	RPO compliance
Server_W2K3_SP2_x64	✓ OK	Test failover	● Compliant
finance08-Recovery	In progress...	Recovering...	● Compliant
fserver	⚠ RPO exceeded	Failover	● Exceeded (1.3x)
Servier RGYD6	✓ OK	Standby	–
Server_W2K8x64_SQL	✓ OK	Ready for failback	● Compliant
fserver	✓ OK	Running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

New Disaster Recovery section

Reduce management overhead

Find all disaster recovery controls in the new Disaster Recovery section.

Manage key functionality using separated tabs: server list, runbooks, connectivity settings, and the credentials store.



□	Name ↑	Status
□	Server_W2K3_SP2_x64	✓ OK
□	finance08-Recovery	In progress...
□	fserver	⚠ RPO exceeded
□	GNM_4576-R4 - recovery	✓ OK
□	Server_W2K8x64_SQL	✓ OK
□	fserver	✓ OK

Original machine: GNM_4576-R4

Recovery server

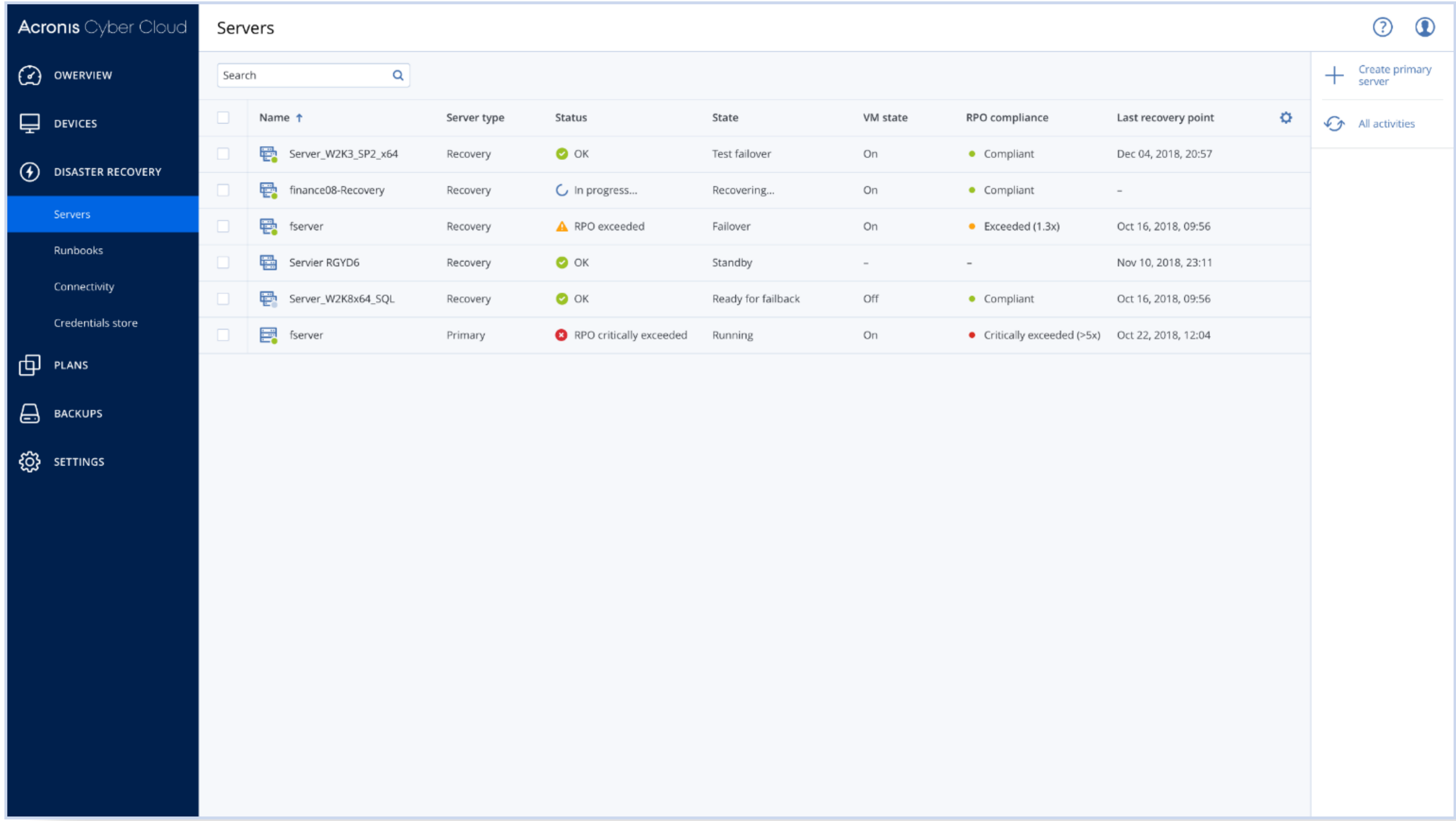
Name	D1-W2012R2-111 - recovery
Status	✓ OK
State	Standby
CPU and RAM	1 vCPU, 4096 MB RAM, 2 Points
Last recovery point	Nov 20, 06:52 PM
IP address	192.168.1.54
Test IP address	192.168.1.61
Internet access	Disabled
RPO Threshold	2 Hours

Redesigned cloud server management UI

Gain greater visibility into your cloud server environment

Improvements in the cloud server management interface:

- Device statuses are now more informative and actionable, and based on alerts.
- The “Machine status” column is still in the table but is now called “State”.
- A new “VM state” column is added.
- The “Backup status” column is replaced with a more informative “Last recovery point” column.



Name	Server type	Status	State	VM state	RPO compliance	Last recovery point
Server_W2K3_SP2_x64	Recovery	OK	Test failover	On	Compliant	Dec 04, 2018, 20:57
finance08-Recovery	Recovery	In progress...	Recovering...	On	Compliant	–
fserver	Recovery	RPO exceeded	Failover	On	Exceeded (1.3x)	Oct 16, 2018, 09:56
Servier RGYD6	Recovery	OK	Standby	–	–	Nov 10, 2018, 23:11
Server_W2K8x64_SQL	Recovery	OK	Ready for failback	Off	Compliant	Oct 16, 2018, 09:56
fserver	Primary	RPO critically exceeded	Running	On	Critically exceeded (>5x)	Oct 22, 2018, 12:04

Acronis

For additional information, please visit **www.acronis.com**