Acronis® Backup & Recovery™ 11

Next Generation Physical, Virtual, Cloud Backup, Disaster Recovery, and Data Protection Solution from Acronis

An Acronis White Paper

Table of contents

Executive Summary

Information sprawl continues. It's been the case for so long that it barely seems newsworthy. Information isn't just growing - it's exploding out of control. At the same time information has always been important, but rarely could the loss of information damage or even destroy your business like it can now.

Acronis is one of the early and leading pioneers in bringing affordable, high quality backup and disaster recovery to small and medium businesses. Acronis has continually expanded the backup and recovery capabilities they provide through successive technology generations. Acronis has continued to move high end functionality, usually found only in expensive enterprise software, into products affordable for the small and medium business.

Many features of Acronis® Backup & Recovery™ 11 were built to help companies fight uncontrolled growth of storage demands while addressing reliability issues. With **Acronis Backup & Recovery 11**, Acronis continues this trend, **merging disaster recovery and data protection into a single integrated product** and simplifying and standardizing backup and recovery processes into easy-to-follow procedures.

Acronis Backup & Recovery 11 enables organizations to recover entire Windows®, Linux® or virtual systems in minutes, not hours, backup, catalog, find and recover application[1] databases, such as Microsoft® Exchange Server or Microsoft SQL Server™, or even individual e-mails.

Acronis Backup & Recovery 11 comes in different editions to suit the needs of small, medium and large organizations. Starting from extremely lightweight and easy-to-use products designed to back up individual workstations, servers or virtualization hosts and growing to a full-scale unified solution for **disaster recovery and data protection** across **physical, virtual and cloud**.

> **❝**
> *...The Gartner Group[2] projects that a companies' average data storage requirements are rocketing upward by 60-70% annually"*

New Features in Acronis Backup & Recovery 11

Acronis Backup & Recovery 11 is the next generation data protection and disaster recovery solution from Acronis. Data protection has been added to Acronis Backup & Recovery 11 because of the increasing demands to retain multiple copies of compliance and other critical information in online and offline storage as well as to provide privilege-based access to that information.

1. Applications support comes in upcoming releases
2. Best Practices for Addressing the Broken State of Backup, Gartner, 2010

Data Protection and Disaster Recovery in a Single Solution

To ensure high performance backup and recovery, Acronis Backup & Recovery 11 captures entire disk images and saves them into **disk-based** storage such as SAN, NAS or direct attached storage, optical media, **tape** or even **cloud storage**. If a disaster occurs, an image can be rapidly restored to the same or different **physical or virtual** machine and even to **dissimilar hardware**.

Images may also be catalogued to enable fast and easy search for and recovery of files, entire application databases, such as Microsoft Exchange Server or Microsoft SQL Server, or even individual application items, such as e-mails. Integrated, full-featured application-aware backup and recovery of files and applications makes Acronis Backup & Recovery 11 a unique solution **combining data protection and disaster recovery in a single integrated product**.

Catalog and Search

The most complicated part of data protection is not back up. Rather, it's recovery from a backup. Acronis Backup & Recovery 11 catalogs backups and displays them in a single unified view to help administrators easily browse and manage data in backups across all locations, down to specific versions. Search capability enables a specific, needed piece of information to be found and recovered.

Staging and Multi-Destination

To leverage maximum cost-saving, older backups can be automatically moved to cheaper storage, such as tape or low cost disk. Backups can also be stored in more than one location for increased redundancy. Some or all backups from a remote office can be copied across a Wide Area Network or saved on tape to be shipped offsite manually. Source-level deduplication for the remotely located machines enables backups to be run over a Wide Area Network using the minimum amount of bandwidth possible.

Cloud storage makes reliable off-site backups available to small business or remote branch offices with nearly zero initial investments in hardware or software licenses and eliminating the need for removable physical disk or tape storage devices.

Acronis® Universal Restore™ for Linux

The Acronis® Backup & Recovery™ 11 Universal Restore™ option enables organizations to use dissimilar hardware for standby purposes eliminating the need to provision identical hardware for recovery. The Acronis Backup & Recovery 11 Universal Restore is now available for both Windows and Linux.

Acronis Universal Restore also has additional functionalities. It enables a device driver to be applied to a Windows or Linux operating system already on the disk. This eliminates the need to perform backup and restore to fix the operating system when hardware is replaced or a system hard disk is physically moved to another machine. It also enables another dissimilar Linux system to be used as disaster recovery platform for the production system.

Disaster Recovery Plan

Acronis Backup & Recovery 11 may be configured to automatically generate a Disaster Recovery Plan document each time a backup is run with complete, direct and easy-to-follow instructions. The Disaster Recovery plan can be combined with other disaster recovery procedures as part of a Business Continuity plan for protecting critical IT infrastructure and business processes.

Meeting Recovery Time Objectives

Backup and recovery preparations entail two significant challenges - backup performance and Recovery Time Objective (RTO). RTO is the maximum time allowed to recover a system after a failure. Meeting Recovery Time Objective requires careful planning considering the different factors that might affect it.

Different disaster types require different ways to recover. Recovery procedures can range from needing to quickly find and recover an individual file or e-mail to rebuilding an entire system, or even a site, on a bare metal hardware, for example if the site were affected by a natural disaster. Acronis Backup & Recovery 11 addresses the entire range of needs, in one solution.

Data Recovery versus System Recovery

Many organizations only perform data backup. It might consist of a simple folder-to-folder copy over the network, or escalate all the way to complex client-server architecture with disk and tape storage systems on the back end. Some of these solutions only back up application data. Others also back up the files related to the operating system. However, a backup copy of the operating system files is not a disaster recovery solution, in which fast and consistent recovery in case of complete system failure can be carried out.

There are two main goals to confidently meet a Recovery Time Objective:

1. Recover the operating system and application to a consistent running state.
2. Recover the required copy of data back into the system.

The usual way to recover a system requires IT to re-install the operating system and applications, especially the backup application before data can be recovered. Then, patches and application configurations are installed and configured. The entire process can take several hours or even days before the first byte of data are restored. This mostly manual process requires significant expertise to install the backup application and configure it to work with the existing backup infrastructure.

In today's fast-paced business environment, a disaster recovery solution that simplifies and automates the process is needed so that the system can be recovered quickly. Acronis Backup & Recovery 11 enables IT to recover a system and its applications to a consistent state in less than an hour, with a few simple steps. Acronis' patented imaging technology allows complete system recovery without the need to re-install and re-configure the backup application. All system and application settings are recovered to the state at which the backup was done.

In addition, Acronis Backup & Recovery 11 provides functionality to find and recover individual pieces of data, such as files or e-mails, either from disk-image backup or special file- or application- level backup.

With Acronis Backup & Recovery 11's ease-of-use, backup configuration and recovery can be carried out by any IT staff, freeing highly-skilled IT resources from recovery related tasks.

Recovering to Dissimilar Hardware

Recovering a system onto dissimilar hardware from a failed system often results in a failed recovery. Due to the differences in hardware and drivers, the system usually cannot start normally after a full restore. Highly-skilled systems engineers are needed to carry out procedures such as copying and replacing drivers, editing and creating Windows Registry keys. Often, this tedious, error-prone process requires hours or even days to complete, threatening business continuity.

Acronis Backup & Recovery 11 Universal Restore is an option that solves the problem quickly. It simplifies and streamlines the recovery process for dissimilar hardware restore. With Acronis Universal Restore, systems can be recovered to dissimilar hardware in minutes, not hours or days. Drivers for the new hardware can be added to the recovery. Acronis Universal Restore will automatically configure the underlying operating system settings so that the recovered system will run on the new hardware.

Human Factors in Disaster Recovery

Recent major disasters throughout the world have taught us new lessons about disaster recovery (DR). Organizations impacted by these disasters learned that the disaster recovery plan they anticipated would suffice, could not or did not work according to plan.

Many of the impacted organizations had to perform the recovery at the DR site without the personnel responsible for it, because these people were also adversely impacted by the disaster. They learned that recovery should not be dependent on the selected few IT staff members that have special knowledge of the systems and the technical know-how to recover them.

To be sure that existing staff can handle a disaster; the recovery process must be as simple to operate as is technologically possible. Any time spent looking for operating system and application CDs, license keys, or reviewing system and network documents will delay recovery of line-of-business processes by hours or even days.

The Disaster Recovery Plan automatically generated by Acronis Backup & Recovery 11 can be used by anyone that actually performs the disaster recovery, not just by the people who were trained to do it.

Shrinking RTO with Instant Restore™
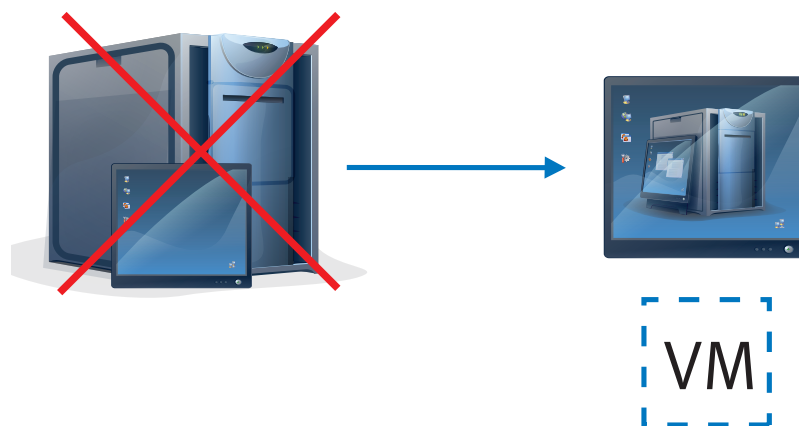
P2V recovery using Instant Restore

Acronis Backup & Recovery 11's Instant Restore feature enables recovery to a standby virtual machine that has been incrementally updated to be a replica of the production server.

For most applications, having a replica instead of a backup isn't adequate because if destructive changes may have already been replicated there is now no way to recover from the replica. With Acronis Instant Restore the virtual machine is updated from the backup archive when the backup completes. This combines the advantages of a backup and replication. It enables the stand-by virtual machine to simply be started if it is known to be good or to be restored from an older backup; avoiding double duty for the production server.

It's also a very economical solution -if the standby virtual machine is hosted on a server that's also used for other applications. The hosting machine would require few or no additional dedicated resources to implement and maintain.

Automated Retention and Staging

Companies balance between challenging RTOs and internal policies or compliance requirements that require retaining backups for extended periods of time. It's simply not feasible to store every daily backup, even incremental, for several years on high performance disk storage that's suitable for fast recovery.

When backups become older, their importance for disaster recovery decreases as well. It's very unlikely that a company will need to use a year-old backup for urgent disaster recovery or that a difference between a 426 and 427 day old backup would make any difference to the recovery process.

Acronis Backup & Recovery 11 can be configured to automatically delete some or all backups when they become too old, or move (stage) them to another, less expensive storage such as tape or lower cost and performance disk (SATA, SAS, etc). Acronis Backup & Recovery 11 enables specifying multiple locations where backups should automatically be moved throughout the backup's lifetime.

Acronis Backup & Recovery 11 also includes templates for industry-standard backup rotation schemes such as Grandfather-Father-Son, and allows the creation of customized schemes tailored to serve all backup scheduling and retention needs.

The configuration of Acronis Backup & Recovery 11 retention and staging is both intuitive and flexible. The reason for that is, unlike competitive products, Acronis Backup & Recovery 11 was initially created as a disk-to-disk backup solution. Disk backup allows much more flexibility than tape backup.

For example, it's much easier to randomly access information or free space by deleting a file in the middle of a disk, than it is to perform the same operations with tape. Most other data protection solutions were initially tape-based, and usually implemented disk-based storage as emulation of tape backup, inheriting all tape's limitations and the resulting difficulty of configuration and management.

Is One Copy Good Enough?

The core goal of a backup and recovery solution is to create and maintain a copy of data to be used for recovery if the primary data source is lost or damaged.

Stringent Recovery Time Objectives usually require a local disk to be recovered fast. However, if the backup copy is in the same location as the production environment, the large scale disaster has likely impacted both. To protect against this scenario, businesses often keep another copy of their data off-site at a geographically dispersed location.

Historically tape backup was an affordable way to ship backups offsite for storage. But, there was no single integrated solution that combined a fast and reliable image-based disaster recovery and and long-term tape-based storage in a single package. Companies were forced to use two different solutions, which increased cost and created numerous management difficulties.

Acronis Backup & Recovery 11 enables backups to be saved to multiple destinations, including to tape. Backups are cataloged, which makes it easy to find out what backups are available where they are stored, search for specific image or item, and initiate a restore.

While tape backup was sufficient for many years, it was certainly never ideal – even for long term data retention. Acronis Backup & Recovery 11 supports several attractive alternatives to tape backup and offsite shipment. These include backup to a remote location over a WAN or to hosted, subscription-based Acronis Online Storage.

Acronis Backup & Recovery 11's incremental backup capability enables only changes that have occurred since the last backup, to be transmitted over WAN, reducing the amount of network bandwidth required for updating a backup. Source-based data deduplication reduces network bandwidth requirements even more by not transmitting identical data more than once.

Together, this reduces backup bandwidth requirements to very acceptable levels and creates an opportunity for small businesses and branch offices to achieve reliable off-site backup all automated without the need to invest in and maintain tape hardware.

Acronis Backup & Recovery 11 multi-destination backup enhances these benefits further. For example, while daily backups are performed locally, only weekly backups might be stored online or shipped off-site, lowering bandwidth and storage requirements even further. Acronis Backup & Recovery 11 takes care of the data encryption, backup types, de-duplication and other details for all of these options.

Data Deduplication and Image Backups

Deduplication is a proven way to tackle the explosive data storage growth issue by eliminating redundant data in a storage system and promising to reduce backup data volume up to 90% or more. Now, administrators can chose to either stretch storage purchases over a much longer period of time or store more data on existing resources.

Acronis Source and Target Deduplication
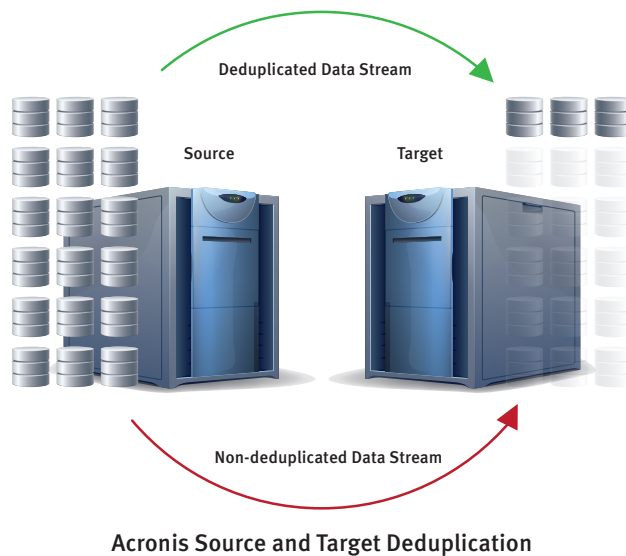
Acronis Backup & Recovery 11 features integrated global software-based deduplication, which makes it affordable for small and medium businesses. Acronis Backup & Recovery 11 deduplication is unique in that it can be applied to files, applications, and disk image backups – which are the most suitable for disaster recovery.

Backup images, however, typically also create the most data redundancy. For example, each of the backups for one hundred Windows machines contain operating system files of about 2GB each that are identical, and would be duplicated one hundred times when backup is taken the first time for every server. If the backup policy is to retain three full backups for every server, the total amount of storage required for the Windows operating system alone for all 100 systems would be around 600GB. Of that amount, only 2GB is actually unique saving 598GB of storage.

After deduplication, only one copy of any duplicated files or blocks within or across these servers will be stored. For user created data such as user home directories, significant duplication of files and blocks may also exist and these duplications will also be eliminated and storage space will be saved.

Acronis' unique data deduplication capabilities allow users to choose between deduplication at the source side or at the target storage side. When source-side deduplication is used, the backup agent performs the deduplication process before transmitting the data to the storage node, reducing bandwidth requirements and enabling remote backup over WAN links.

Acronis Backup & Recovery 11 Deduplication has the following benefits:

1. Eliminates identical blocks of data and saves storage space and cost
2. Supports much longer retention periods on disk, typically 3-6 months
3. Saves network bandwidth, especially when data is being transferred over WAN
4. Minimizes or eliminates tape storage
5. Minimizes manual intervention at the remote sites for tape media management, the need to physically transport backup tapes to central location, and data leakage risks during tape transportation

Managing a Complex Hybrid IT Environment

Virtualization is a proven way to increase server use, reduce footprint and power consumption, and gain IT environment flexibility. Many companies have embraced virtual server technology and consolidated some or most of their physical servers to virtual servers – retaining dedicated physical servers for only the most demanding applications.

With all those advantages, transition to virtual environments also introduces new disadvantages including backup management, disaster recovery and data protection challenges. Traditional backup and recovery solutions don't use virtual resources efficiently and usually force companies to deploy, maintain and manage two different backup solutions - one for physical and the other for virtual.

Acronis Backup & Recovery 11 provides a unified interface for managing physical and virtual machine backup, recovery, and data protection in a common way. This makes Acronis Backup & Recovery 11 an attractive solution for companies that use both physical and virtual machines.

Next Generation Virtual Machine Backup

Acronis Backup & Recovery 11 was designed with virtualization in mind. Acronis Backup & Recovery 11 extends physical machine backup and recovery to virtual environments in a virtualization-aware and efficient way.

Acronis Backup & Recovery 11 provides agentless virtual machine backup. With agentless backup there's no need to have an agent installed on every virtual machine - one agent per physical host or even one per environment is enough. Backups may be done by using VMware's vStorage APIs for Data Protection on an agent located in a special virtual appliance or installed on a dedicated Windows host.

This enables LAN-free backup when no backup data is going through the LAN and enables processing to be offloaded from the virtual machine hosts. Agentless backup is available for VMware ESX(i)®/vSphere® and Microsoft® Hyper-V®.

An Acronis Backup & Recovery 11 Virtual Edition license enables organizations to extend cost-savings and flexibility benefits to their virtual machine infrastructure by protecting all of the virtual machines running on a single physical host with a single software license. The single Acronis Backup & Recovery 11 Virtual Edition license provides virtual machine support for:

- VMware ESX(i)/vSphere
- Microsoft Hyper-V
- Citrix® XenServer®
- Red Hat® Enterprise Virtualization / KVM
- Parallels® Server 4 Bare Metal

Acronis Backup & Recovery 11 is also integrated with VMware vCenter and is VMware® vCloud™ Director tested.
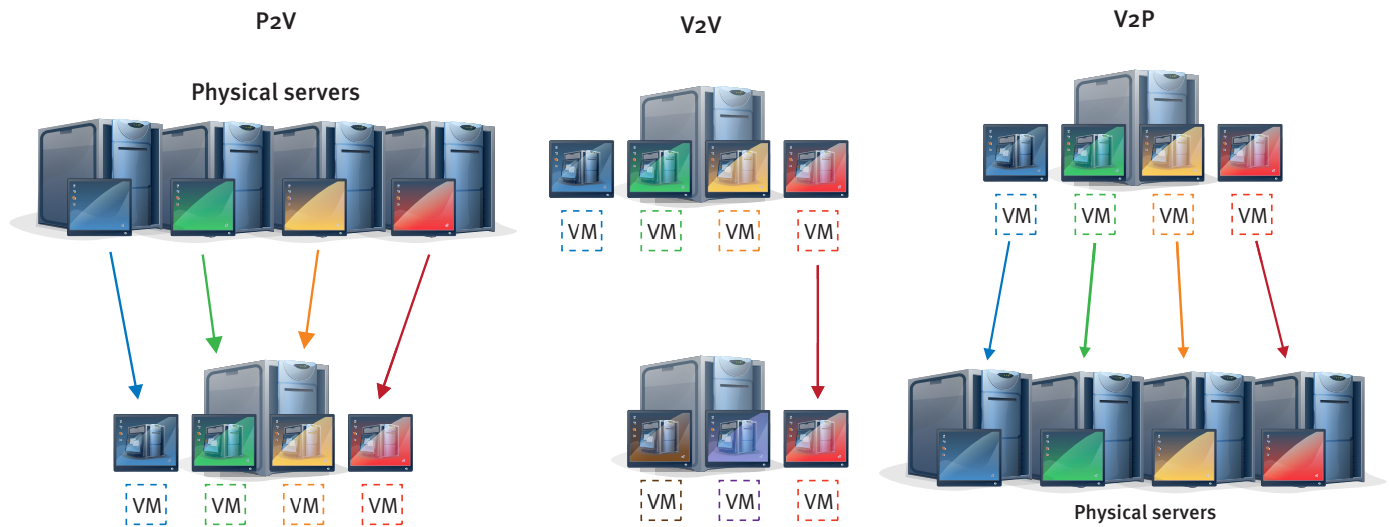
Acronis Backup & Recovery 11 Virtual Edition Server Consolidation and Migration

Server Consolidation and Migration

For server consolidation, Acronis Backup & Recovery 11 Virtual Edition enables rapid conversion of physical servers into virtual machines (P2V). Acronis Backup & Recovery 11 Virtual Edition also supports unlimited virtual server to virtual server migrations (V2V), and rapid restoration or migration of virtual servers back into physical servers (V2P), if the need for dedicated application server arises.

Backups of physical machines may be restored to virtual machines and vice versa, or even between different hypervisors. Combined with Acronis Universal Restore, this provides unlimited possibilities for P2P, P2V, V2P and V2V.

Cloud-based Backup

Acronis Backup & Recovery 11 Virtual Edition combines with Acronis Backup & Recovery 11 Online to enable Virtual to Cloud backup (V2C) and Cloud to Virtual recovery (C2V). Combined with VMware® vCloud™ Director, Acronis Backup & Recovery 11 Virtual Edition enables Any to Cloud backup (X2C) and Cloud to Any recovery (C2X).

The Unified Platform

All Acronis Backup & Recovery 11 functionality is built on a Unified Platform from a common code base, which is unique among competitive backup, restore, and data protection products. This allows a unique level of integration for data recovery and disaster protection of physical, virtual and cloud environments with one platform.

The Unified Platform allows configuring and monitoring backup and recovery throughout an entire system and all components in a single unified way, without a need to learn new product or new concepts every time new technology is introduced in an organization.
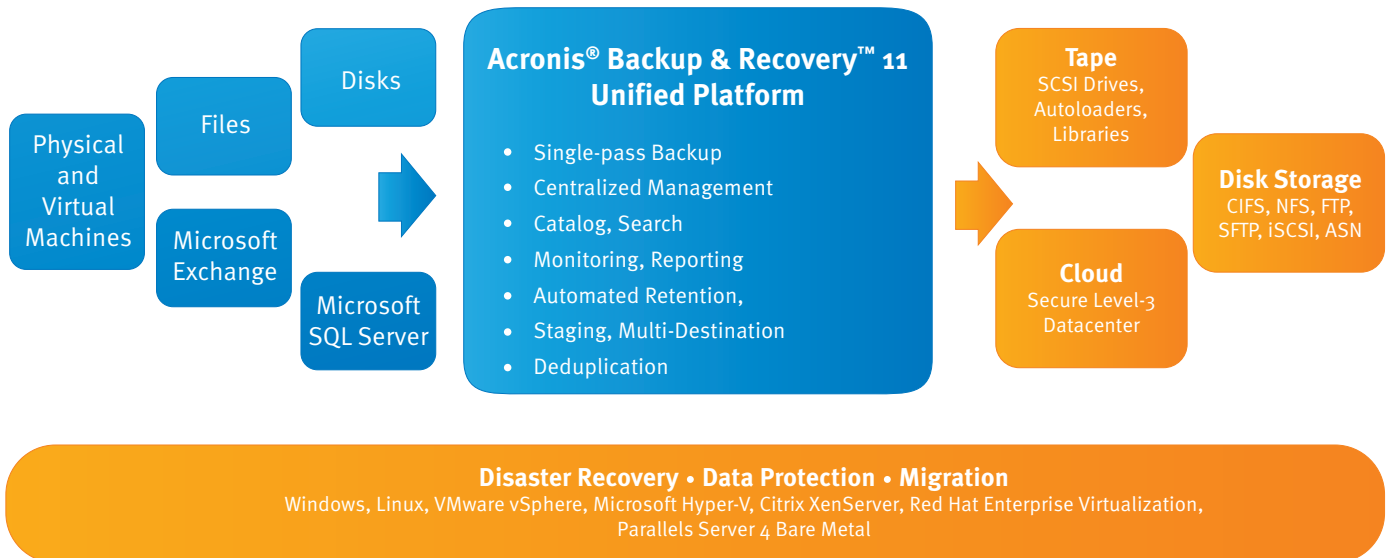
## Scalable Centralized Management

Managing data backup for a large environment can be a time-consuming and tedious task when hundreds or thousands of machines are involved.

Acronis Backup & Recovery 11 centralized management capability, part of the Unified Platform, makes it possible to carry out all backup and disaster recovery operations from a single console, including tasks related to Windows workstations, Windows and Linux servers or virtualized machines on VMware, Microsoft, Citrix, RedHat or Parallels platforms.

Acronis Backup & Recovery 11 is designed to meet the needs of small business users and can scale seamlessly to support thousands of machines.

Acronis Management Server

The Acronis Backup & Recovery 11 Management Server is the central server that drives all data protection and disaster recovery activities within an organization. It provides a single entry point for administrators to manage the entire Acronis Backup & Recovery 11 infrastructure and is the only solution in the industry that provides a common management interface and procedures for Physical, Virtual, and Cloud environments.
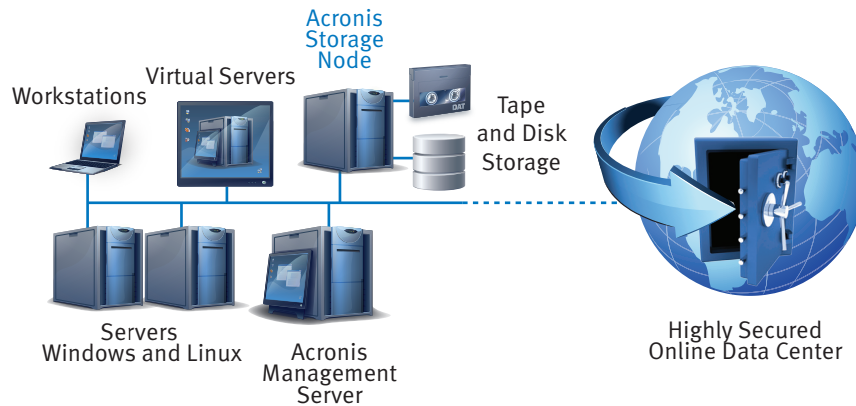
Acronis Backup & Recovery 11 Managing a Hybrid Environment

All managed machines, physical or virtual, are registered to the Acronis Management Server. Groups can be created to organize managed machines into logical groups to facilitate management and reporting at group level. Physical or virtual machines can be added to the groups either manually or automatically based on defined criteria such as operating system, IP address range or organization unit. The Acronis Management Server can also be used to configure, monitor and manage all backup plans and tasks across the environment.

Centralized backup plans eliminate the need to create backup tasks on each individual machine. Instead, a standard plan can be created and applied to a number of machines, or groups of machines, saving time and avoiding backup configurations that deviate from a backup policy that an organization may already have in place. For example, a centralized backup plan can be created for full backups of all servers belonging to finance, specifying the backup destination, retention requirement and day and time the backup should run.

Centralized backup plans can greatly reduce the number of backup tasks that an administrator needs to individually maintain in the system. Without it, administrators may have to define and manage thousands of individual backup tasks for an environment with thousands of managed machines. The management server also maintains a centralized repository that tracks the results of all activities within the Acronis Backup & Recovery 11 infrastructure.

Based on the data collected, reports may be generated and displayed in a web browser. There are several pre-define report types, each of which can be customized. Reports may be run on physical and virtual machines with their statuses, backup plans and tasks, including history of their execution, vaults where backups are stored, archives and backups.

For customization and integration flexibility all reporting information is stored in a Microsoft SQL Server database with an open and documented format.

Even though a given set of machines may be managed by only one Acronis Management Server at a time, which itself might be affected by disaster, it is not a problem because schedules are controlled by individual machines independently of the management server, and backups, restores and most other activities will continue to run. Even if the management server is not available it is possible to connect to individual machines to change their configuration, manage tasks or initiate restore. Other solutions usually require expensive clusters to fulfill similar level of reliability.

Acronis Storage Node

Acronis Storage Node performs the role of controlling and optimizing backup storage resources. It reduces the workload on managed machines by taking over service tasks such as cataloging, backup retention, consolidation, validation and staging which would otherwise consume resources on the managed machines.
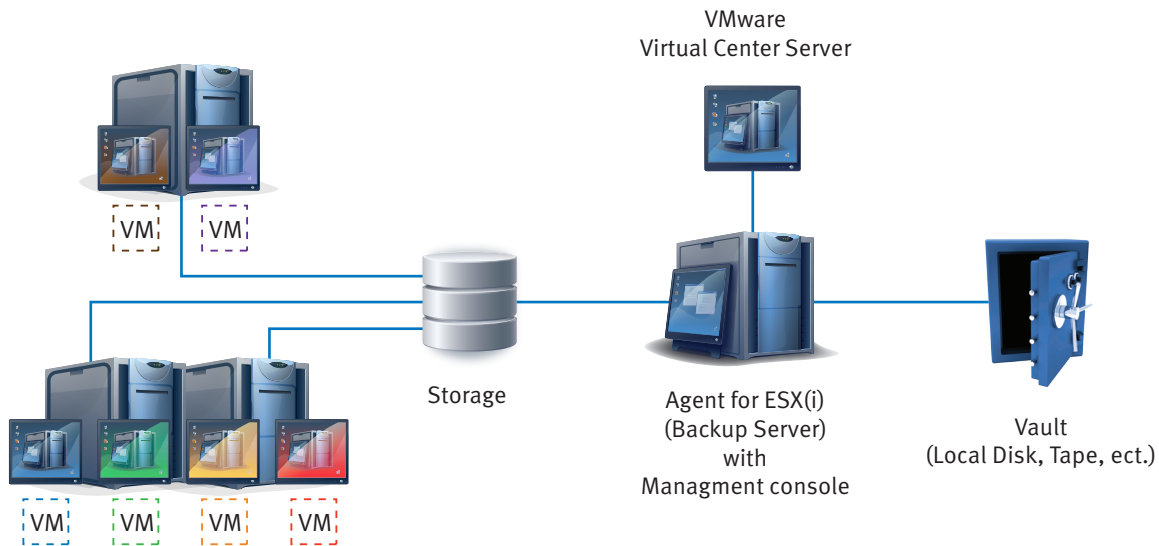
Backup traffic going from agents directly to storage nodes

The storage node is a key to creating a highly flexible and scalable infrastructure. With it, administrators can add storage resources whenever more capacity is needed. It supports devices such as local disks, shared network folders and NAS, SAN attached disks and tape libraries. Storage nodes are usually located near the managed machines they protect and can be managed by the Acronis Management Server anywhere on the network.

The Acronis Backup & Recovery 11 catalog is also held by the storage node making it easy to find a version of the file or other item to restore across all locations. The Acronis Storage Node also enables backup deduplication. By detecting and eliminating duplicated files and blocks, deduplication can typically reduce storage capacity consumption by as much as 90%.

To ensure backup image security, backup images can be either encrypted by the managed machine or the Acronis Storage Node.

A single Acronis Backup & Recovery 11 domain can scale up to 50 Acronis Storage Nodes with every storage node managing 20 disk/tape vaults, all managed by one Acronis Management Server. Backup data is transmitted directly from the managed machines (backup agents) to the Acronis Storage Nodes and saved into the vaults.

Acronis Backup & Recovery 11 Management Console

All management and configuration activities are done through the Acronis Backup & Recovery 11 Management Console. From the management console, the administrator can connect locally or remotely to Acronis Management Server or individual machines to perform backup and recovery operations. It is highly intuitive and can be operated without training.
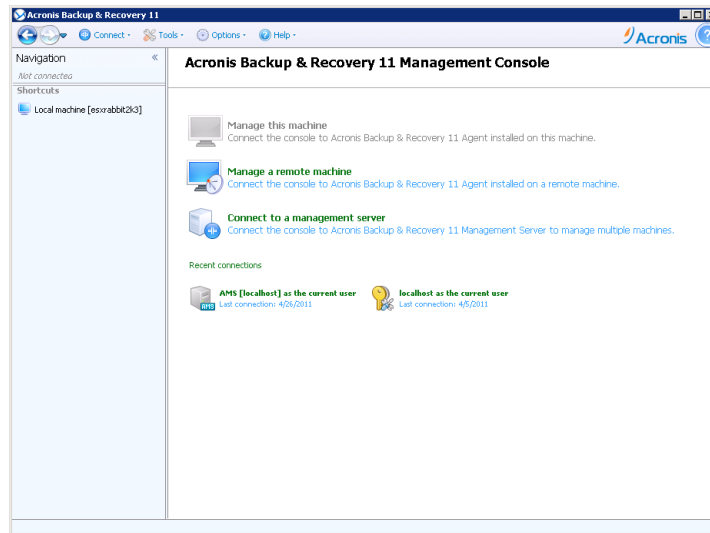

Managed vaults are created under a storage node and configurations such as deduplication, encryption and storage settings can be specified. The administrator can also drill down into backups that exist in the vault and initiate tasks such as validation and cleanup.

From the console, all running activities are listed, and an administrator can monitor all progress and terminate activities. Task history and logs enable the administrator to perform advanced troubleshooting on failed jobs.

Alerts view gives a consolidated list of issues requiring administrator's attention and helps to identify the hotspots. Rectifying actions can then be prescribed in the shortest possible time.

Acronis Backup & Recovery 11 Management Console includes a dashboard that provides a high-level status view of the entire backup and recovery infrastructure. The dashboard is the perfect tool for operation management to quickly get a status snapshot of the entire backup infrastructure.
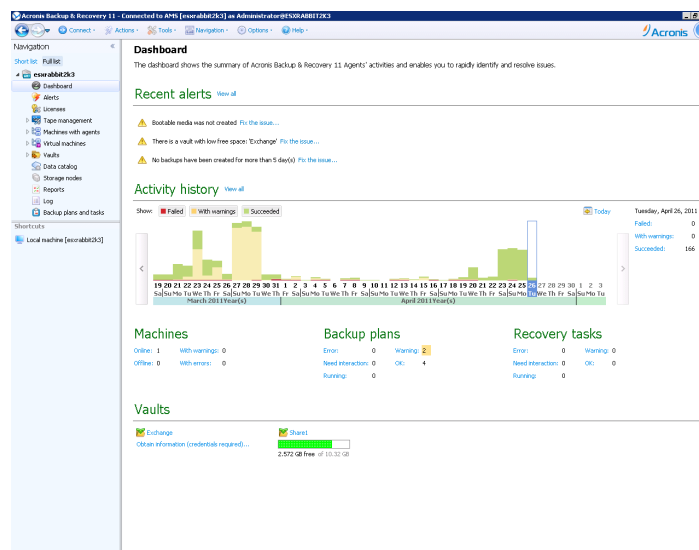
Remote Recovery

Organizations performing remote office and workstation/laptop backups also appreciate the convenience of performing a remote recovery, as it costs time and money to send IT staff to remote locations for that purpose. Remote restores eliminate the need to travel to a remote location to recover a machine efficiently – impacting RTO. In certain cases, remote recoveries are the only viable option for security reasons.

A remote machine can be booted through network boot (through Acronis PXE Server), from the Acronis Recovery Media or the Acronis Startup Recovery Manager via the boot prompt. Once the agent is running, a connection can be remotely established from the management console and the remote administrator can execute the recovery tasks.

Conclusion

Acronis Backup & Recovery 11 also provides comprehensive Physical, Virtual, and Cloud environment backup, recovery and data protection in a common framework using the same management and implementation interface across all environments. Compared to competitive products that require 2 or 3 different products for Physical, Virtual, Cloud environments, Acronis Backup & Recovery 11 can reduce your backup, recovery, and data protection Total Cost of Ownership (TCO) by up to 100-200% per annum through reduced training and operating costs.

Acronis Backup & Recovery 11 is engineered to provide simple and cost-effective data protection and disaster recovery to organizations of all sizes. It enables organizations to standardize disaster recovery procedures easily across their physical, virtual and cloud environments. It enables reducing Recovery Time Objectives from typically 4hrs to less than 1hr and to nearly instant when using Acronis Instant Restore. This greatly reduces the need for expensive clustering solution for most applications.

Acronis Universal Restore technology simplifies restoration of Windows, Linux and Virtual Machines onto dissimilar hardware platforms with procedures similar to standard Acronis recovery procedures, enabling staff with only basic IT training to perform recoveries.

Acronis Backup & Recovery 11 optimizes storage resource with automated retentions and staging and with its integrated backup deduplication engine and effectively reduces storage requirements by 90% or more. Deduplication also minimizes the volume of backup data traffic transmission through the network enabling remote office backup over the WAN. The backups can be staged and sent to different locations throughout their lifecycle or sent to additional locations or to online storage to provide an added layer of data protection.

With enterprise-class scalability, Acronis Backup & Recovery 11 infrastructures are able to grow on-demand to handle increased workloads. Startup cost with Acronis Backup & Recovery 11 is minimal and organizations only invest in more infrastructure when needed. As the environment grows, centralized management capability is maintained, while centralized backup plans ensure that the number of backup tasks remain manageable.

With Acronis Backup & Recovery 11, organizations can now build a backup and recovery infrastructure that is scalable, cost-effective, resource optimizing and easily manageable; and meet Recovery Time Objectives and disaster recovery objectives with ease.

About Acronis

Acronis is a leading provider of easy-to-use disaster recovery and data protection solutions for physical, virtual and cloud environments. Its patented disk imaging technology enables corporations, SMBs and consumers to protect their digital assets. With Acronis' disaster recovery, deployment and migration software, users protect their digital information, maintain business continuity and reduce downtime. Acronis software is sold in more than 90 countries and available in 14 languages.

For additional information, please visit www.acronis.com. Follow Acronis on Twitter: http://twitter.com/acronis.

For additional information please visit http://www.acronis.com

To purchase Acronis products, visit **www.acronis.com** or search online for an authorised reseller.

Acronis office details can be found at **http://www.acronis.com/company/worldwide.html**

Acronis®