Acronis

acronis.com

Acronis Cyber Protect 15

Best Practices

REVISION: 2/12/2024

Table of contents

Copyright statement

DOCUMENTATION IS PROVIDED “AS IS” AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID.

Third party code may be provided with the Software and/or Service. The license terms for such third-parties are detailed in the license.txt file located in the root installation directory. You can always find the latest up-to-date list of the third party code and the associated license terms used with the Software and/or Service at https://kb.acronis.com/content/7696

Acronis patented technologies

Technologies, used in this product, are covered and protected by one or more U.S. Patent Numbers: 7,047,380; 7,246,211; 7,275,139; 7,281,104; 7,318,135; 7,353,355; 7,366,859; 7,383,327; 7,475,282; 7,603,533; 7,636,824; 7,650,473; 7,721,138; 7,779,221; 7,831,789; 7,836,053; 7,886,120; 7,895,403; 7,934,064; 7,937,612; 7,941,510; 7,949,635; 7,953,948; 7,979,690; 8,005,797; 8,051,044; 8,069,320; 8,073,815; 8,074,035; 8,074,276; 8,145,607; 8,180,984; 8,225,133; 8,261,035; 8,296,264; 8,312,259; 8,347,137; 8,484,427; 8,645,748; 8,732,121; 8,850,060; 8,856,927; 8,996,830; 9,213,697; 9,400,886; 9,424,678; 9,436,558; 9,471,441; 9,501,234; and patent pending applications.

Introduction

About this guide

This document describes Acronis Cyber Protect best practices and recommendations for a number of typical environments, which will help you to avoid common problems tied to misconfigured deployments.

Recommendations for each environment are self-contained; simply choose which one corresponds best to your scenario.

Recovery recommendations, the Miscellaneous recommendations section and the Appendices are not specific to the described environments and should be followed by anyone using this guide.

Intended audience

This guide is intended for backup administrators or consultants managing Acronis Cyber Protect.

Most sections of this guide assume you already have hands on experience with Acronis Cyber Protect, and will serve as an "advanced user guide", meaning that more basic usage information must be found in Acronis Cyber Protect User Guide.

The information in this guide is based on the experience gained by the Acronis engineers while resolving customer issues with Acronis Cyber Protect. For best results, it is advised to follow the whole set of recommendations corresponding to your environment type.

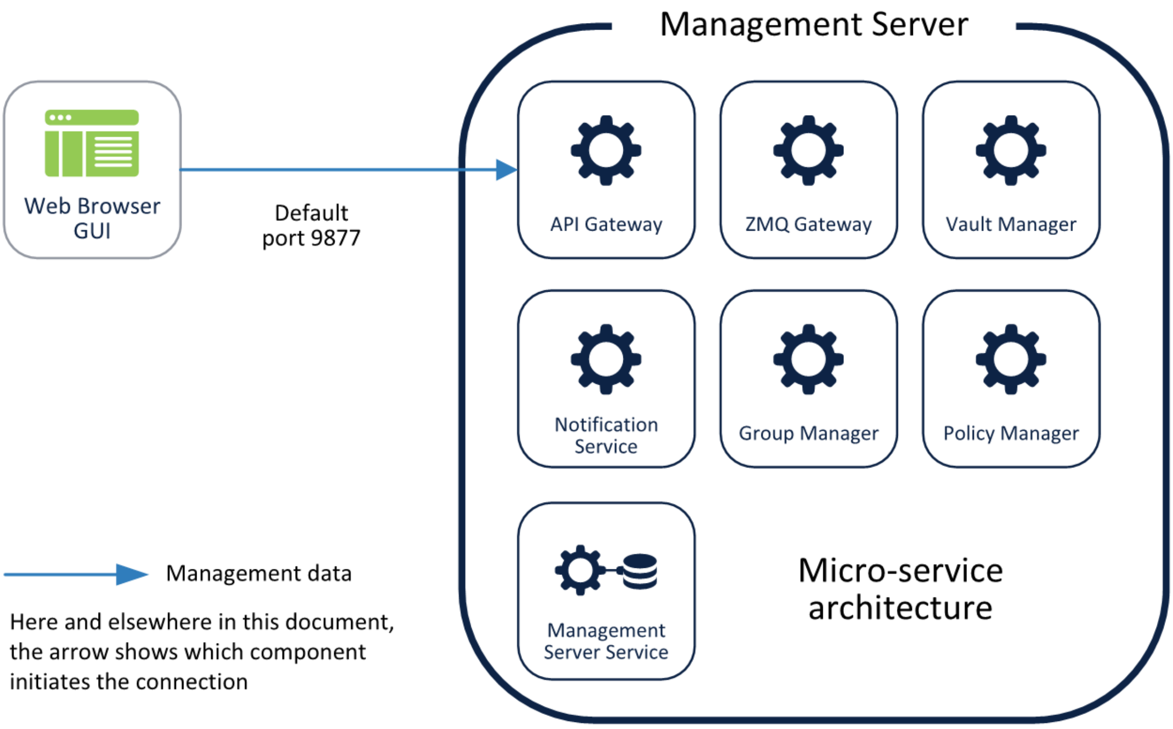
- Single and isolated machines
- Small environments
- Typical SMBs
- Large environments

Acronis Cyber Protect components and architecture

Acronis Cyber Protect consists of the following installable components.

Management Server

Cyber Protect Management Server is composed of a number of services responsible for management functions of Acronis Cyber Protect and providing the Web UI. These services manage agents, groups and protection plans; send notifications; collect data, build and save reports, etc. For the list of services and their functions, see Appendix A. The Management Server component is typically installed first and will be your entry point into managing your Acronis Cyber Protect infrastructure. It does not actually participate in any backup, recovery or other data-manipulation operations.



Here and elsewhere in this document, the arrow shows which component initiates the connection

Components for Remote Installation

This is an archive of all the installation components found in the full Acronis Cyber Protect installation executable. You need to install it in order to be able to push deploy agents remotely from the Cyber Protect Management Server. If you do not need remote installation functionality from the product GUI, do not install this component in order to conserve space.

Scan Service

Performs antimalware scan of backups in a cloud storage, a local or a shared folder. Scan Service requires Microsoft SQL Server or PostgreSQL Server database. Scan Service is incompatible with the default built-in SQLite database. If you select the SQLite database during the installation, then the following functionality will be hidden in the web console:

- Backup scanning plans
- Backup scanning details widget
- Corporate whitelist
- Safe recovery
- The Status column in the list of backups

Thus, if you need the functionality listed above, customize the installation settings and define the Microsoft SQL Server or PostgreSQL Server databases for the management server.

Protection agents

Acronis protection agents are also installed as a number of services responsible for performing the specific backup, recovery, replication and other data-manipulation tasks on the machines you want to protect. They are typically installed on each device that requires protection and then added to the Cyber Protect Management Server.

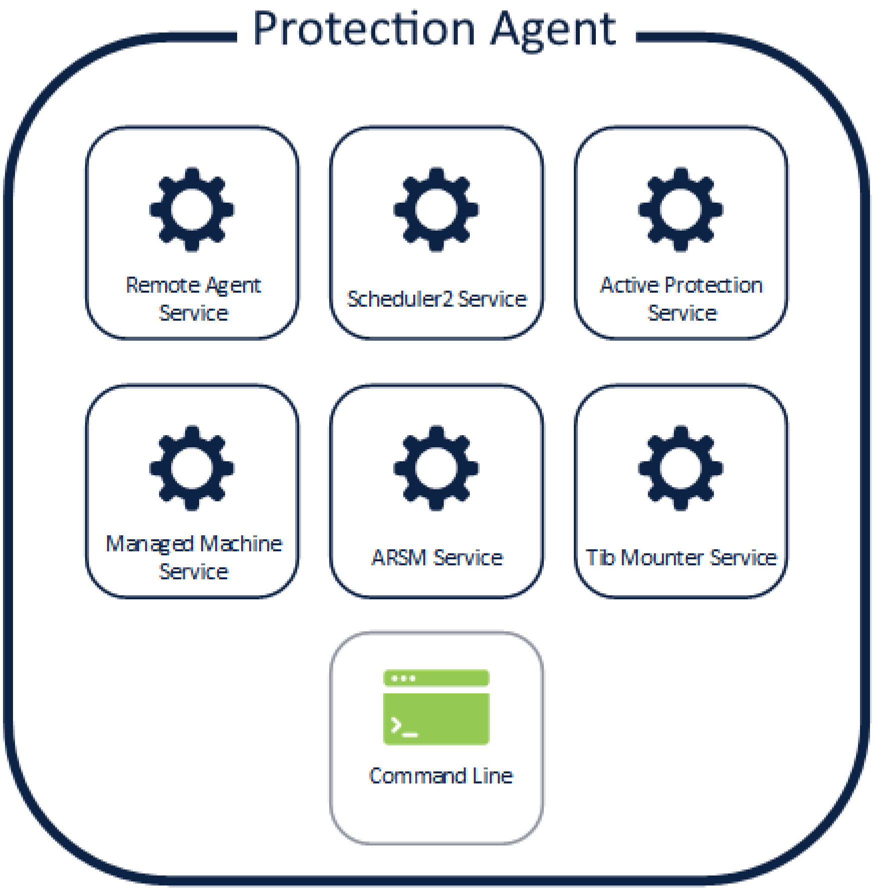
However, Acronis agents are able to work completely independently and do not require constant communication with the Management Server to run their scheduled backup operations. It is also possible to install an isolated agent and forgo the Management Server entirely, although in this case it will have to be managed through the command line.

Different agent types are used to protect different data sources, but they all share the same architecture, communication protocols and the vast majority of the functionality.

You can find the list of currently available agents below.

- Agent for Windows
- Agent for Linux
- Agent for Mac
- Agent for VMware (Windows)
- Agent for VMware (Virtual Appliance)
- Agent for Hyper-V
- Agent for Scale Computing HC3 (Virtual Appliance)
- Agent for Exchange
- Agent for SQL
- Agent for Active Directory

- Agent for Office 365
- Agent for Oracle



Bootable Media Builder

This is a separate GUI tool used to create the two different types of Acronis Bootable Media: the default Linux-based media and the WinPE-based media.

You typically need to install only a single instance of this tool on one of your machines as the media created on one machine will work on others.

The Acronis Bootable Media is an entirely self-contained tool with backup and restore functionality provided by an agent very similar to the ones described above. It allows you to restore any system from bare metal as long as you have the media itself and the file that contains your backup.

Cyber Protect Monitor

This component is installed along with an agent and provides basic interaction with the agent from the system tray or menu bar of your operating system. Using the Cyber Protect Monitor, you can check or stop a running backup directly from the machine on which the agent is installed.

Storage Node

This component provides a managed centralized storage location that agents can use as their backup target. It is required for cataloging, centralized tape backups, and deduplication.

Catalog Service

The catalog service indexes all your backups to enable search and recovery of files inside the backups. It is not required for file restore, only for search.

PXE Server

This service works in conjunction with the Bootable Media Builder and allows you to use the bootable media for booting over the network.

Architecture overview

Acronis Cyber Protect shares its architecture and code base with Acronis Data Cloud, the Acronis cloud platform, which allows service providers to offer backup and other services. This means that the same management components as listed in the beginning of this section are running in our data centers, scaling to thousands of Acronis customers and partners managing 100+ petabytes of data. The major difference being the fact that the services used in the cloud are manually deployed and maintained by a dedicated team on a complex network of servers inside our data centers instead of having these components packaged in a simple single-click installation package as is the case with Acronis Cyber Protect.

The vast cloud service scale of the cloud platform is what determines many architectural decisions that underpin Acronis Cyber Protect. For example, the move from monolithic services using RPC connections in previous products to a more flexible micro-service architecture that communicates using a RESTful API. The choice to use a Web console interface is also made, because this is the best option for providing a UI for cloud services.

The benefit this brings for locally deployed Acronis Cyber Protect customers is also largely tied to scalability and stability at scale. Instead of managing hundreds of end-points, the new Management Server is able to manage thousands of agents effectively even with relatively modest hardware.

The rapid growth of our cloud services platform necessitates constant evolution of the underlying architecture. Since our cloud platform shares its architecture, this necessarily means that the Acronis Cyber Protect architecture is also subject to the same changes.

Resource usage calculator

We created a resource usage calculator as an addition to this guide and reference it regularly throughout. This calculator will help you with hardware sizing of larger environments, but will also help with estimating the storage requirements you would need for the retention periods you specify and the time required to push this data through the network.

The calculator will be regularly updated as we receive feedback and new data. You can always find the latest version of the calculator on the following link.

https://go.acronis.com/resource-usage-calculator

To use this calculator, input the numbers that describe the size of your environment on the first sheet; your protection plan, backup windows, storage you plan to use on the second sheet and check out the resulting recommendations on the subsequent sheets. If you're unsure about using a feature like cataloging or deduplication, read the recommendations appropriate to your environment in one of the sections below.

Licensing

Acronis Cyber Protect 15 editions and licensing

Acronis Cyber Protect 15 is available in the following editions:

- Cyber Protect Essentials
- Cyber Protect Standard
- Cyber Protect Advanced
- Cyber Backup Standard
- Cyber Backup Advanced

For detailed information about the features included in each edition, refer to "Acronis Cyber Protect 15 Editions Comparison including Cloud deployment".

All editions of Acronis Cyber Protect 15 are licensed by the number of protected workloads and their type (workstation, server, and virtual host). Cyber Protect editions are only available with subscription licenses. Cyber Backup editions are available both with subscription and perpetual licenses. For more information about the available licensing options, refer to https://www.acronis.com/company/licensing.html.

To manage the licenses in your environment, in the Cyber Protect web console, go to **Settings** > **Licenses**.

You can also manage the licenses on a per-machine basis. To do so, in the Cyber Protect web console, select the desired machine, and then go to **Device** > **Details** > **License**.

Perpetual license keys for version 15 cannot be used with backup agents from Acronis Cyber Backup 12.5. However, these agents will continue working with their old license keys, even when their management server is upgraded to version 15.

Backup subscription licenses can be used with version 12.5 agents, even when the agents are upgraded to version 15. Cyber Protect subscription licenses can be used only by version 15 agents.

Note
The features vary between different editions. Some of the features described in this documentation may be unavailable with your license.

License Server

Each Management Server installation includes a License Server component. This component stores the licenses in its own encrypted files and periodically checks the assignment and validity of the licenses added to it. Licenses are added after installation, which implies that the installation file and installation process does not change with different licenses. You cannot yet register a single License Server for multiple Management Servers; this functionality will become available in a future version of Acronis Cyber Protect.

If a machine is added to a Management Server, it is always licensed through the corresponding License Server. Every time an agent comes online (or at least once a day), the license assignment is checked and renewed for each agent registered on the Management Server.

Warning!
If this check fails for 30 days in a row (for example, the machine was offsite and was not able to connect to the Management Server for 30 days), the agent will disable backups on this machine.

If you are using isolated machines that are not connected to a Management Server, the agent can be licensed separately via the command line. In this case, the machine will have to be managed through the command line since the UI is part of the Management Server.

An agent cannot be self-licensed while also being managed through the Management Server.

Using Standard and Advanced licenses on one Management Server

Warning!
We do not recommend using a mix of both standard and advanced licenses on a single Management Server installation.

While it is technically possible to add and use both Standard and Advanced licenses on a single Management Server installation, the user experience is not optimized for this scenario. It can lead to situations that allow you to unknowingly create protection plans that will fail every time due to lack of proper licensing.

Use all standard licenses if you have up to five machines and do not need advanced functionality.

If you have a larger environment or need functionality such as backup to tape or off-host data processing, use all advanced licenses.

Single and isolated machines

Environment description

A single machine installation is one where management is done locally, on the same machine as the one being backed up. This scenario applies if you only have one machine to back up, but also to large environments of isolated machines that cannot be managed remotely.

If you want to use the Web console user interface to manage backups on a machine locally, the management server component must be installed along with the agent. In this case, an isolated machine can run under Linux and Windows, but not under Mac because the management components are not available for Mac.

Another option is to manage this machine from our Management Server in the cloud, but this requires a WAN connection and is not always an option.

The final option is to have a single machine managed through the command line only. This scenario does not require the installation of management components or network connectivity, but you will lack a UI to manage your backups and all management will have to be done through scripting and commands.

Note
This option is only applicable for machines with perpetual licenses, since you cannot assign a subscription license to a single isolated machine using only the command line.

Preparing for deployment

This section covers the requirements and recommendations for Acronis Cyber Protect deployment for environments with single or isolated machines.

Software requirements for single and isolated machines

There are no specific recommendations as long as your systems are supported.

The full system requirements can be found in the User Guide.

If you will manage your single machine from within the operating system, make sure to follow the Management Server requirements, which are stricter than the agent requirements. For example, the Management Server components are not supported for Mac.

If you plan to manage the machine from the command line only, follow the Agents section.

Hardware requirements and sizing

You can find the minimum hardware requirements in the User Guide.

Note

Note that when using local management through the Management Server component, you need to add the Management Server requirements to the agent requirements.

Deployment type

Deployment recommendations are different for protecting a single machine vs. an isolated machine (a machine isolated from WAN or local networks).

Single connected machine

If the machine is connected to the Internet, we recommend using the Cloud Deployment model as the simplest way of creating a backup. In this case, the GUI and management is provided from the Management Server components installed in Acronis data centers. Your single machine will connect to this cloud Management Server through the WAN.

Note that some advanced features of Acronis Cyber Protect are not yet available with the cloud deployment. They will be propagated to the cloud deployments in a future release.

Alternatively, if you need one of these advanced features, or you require more direct control over the management components, install them along with the protection agent.

Finally, if this machine is very tight on resources, you can forgo the management GUI, install just the agent and use our command line to create backups via scripts.

Isolated machines

To protect a number of isolated machines that cannot be connected to the WAN or to each other, we recommend installing just the agent and using its command-line interface for management purposes.

The benefit of this approach is that the same script can be used on all the machines to automate the backup process instead of having to manage them directly one-by-one through the GUI of each agent.

For commands description, see the Command-Line Reference Guide.

You can, of course, install the full Management Server component on each isolated machine. This is useful if each machine is going to be managed by its user directly or if you are not comfortable using the command-line approach.

Components and installation

Management components

Install the management components only if you want to manage your single machine using a web GUI running on the machine itself.

In this case, the following components are recommended for installation:

- **Management Server** is required for showing the GUI.
- **Bootable Media Builder** has to be installed on at least one machine in your environment in order to run a disaster recovery if the system is not bootable.

Note
Components below are not recommended for this environment type.

- **Scan Service**
  This component performs antimalware scan of backups in a cloud storage, a local or shared folder. Scan Service requires Microsoft SQL Server or PostgreSQL Server database.
- **Components for Remote Installation** (Windows only)
  This component will allow you to push install Windows agents remotely from inside the GUI of the product. This function is irrelevant when using a single machine.
- **Acronis Storage Node**
  This component is only used when multiple machines create backups to a single storage. This is not used for a single machine.
- **Catalog Service**
  The catalog service is used exclusively for search inside backups when using the storage node.

Protection agents

Protection agents need to be installed on each machine you wish to protect.

For instructions on how to install each agent type, refer to the User Guide.

The protection agent by itself is enough to do all the backup and recovery operations provided you can manage it.

This can be done via the command line that is always installed along with the agent.

Recommended installation procedure

You can find detailed installation instructions in the User Guide.

When installing on Linux, make sure that the required packages are installed first.

Management via GUI

Below are our recommendations if you want to use the web console to manage the agent:

1. Register your product in your Acronis account. Detailed instructions are here: https://kb.acronis.com/content/4834.
2. Download the full installation file appropriate to your operating system, Windows or Linux. Files can always be downloaded from your account after they are registered.
3. Install the Cyber Protect Management Server, Protection agent, Bootable Media Builder on the machine.

4. Import and assign the license.
5. Configure your storage locations.
6. Configure and apply your protection plans.

Management via the command line

Below are our recommendations if you want to use the command line for management purposes.

1. Register your product in your Acronis account. Detailed instructions are here: https://kb.acronis.com/content/4834.
2. Download the full installation file appropriate to your operating system, Windows or Linux. Files can always be downloaded from your account after they are registered.
3. Launch the installation file using the `--skip-registration` parameter.
4. Choose Protection agent for installation and optionally the Bootable Media Builder if you don't have one on another machine.
5. Assign a license to the agent via the `acrocmd add license --key=<LICENSE_KEY>` command.
6. Create backups using the command line.

Protection plan recommendations

What to back up

You will typically want to back up entire machines using a selection of exclusion rules to remove unwanted data from inside the backup.

You can exclude volumes, specific files or extensions. For example, exclude all .avi files from backup of personal notebooks and desktops.

Different backup sources will also require the creation of different protection plans, at least one for each type of source.

For example, if you want to create a monthly backup of the entire machine and daily backups of your important files, this will require two separate plans on the same machine.

Where to back up

Single machines typically have two main storage options:

- You can store all the backups on the machine itself. For example, each machine can backup volume C:\ to its D:\ drive or to an attached USB drive.
- You can store all backups on the network. We recommend a standard NAS or share sized to fit your backup data at the retention period you require. Check out the resource usage calculator for help calculating the approximate backup size given your environment and retention periods.

Scheduling

The recommended backup schedule will typically depend entirely on the data size of your protected devices and their RPO (recovery point objective) targets. As long as the currently running backup has time to finish before the next one starts, you shouldn't have any problems.

That said, backup does take a non-negligible amount of resources from the machine being protected and this could affect production workloads, especially if they are particularly heavy ones.

Our experience shows that a good basic recommended schedule is to have a daily work day incremental backup running at night after closing hours, with a full backup over the weekend.

It is generally recommended to schedule tasks such as replication and validation separately over the weekend as well, if there isn't enough time to complete them after backup.

How long to keep

Retention periods will often be determined by external policy or compliance rules. You can estimate the size of backups for the retention period by using the resource usage calculator.

If you do not have enough first-tier storage, schedule special replication tasks to move data to a different, cheaper storage solution for long-term retention.

For example, you can replicate the backups to Acronis Cloud or make use of tape storage for long term retention.

Replication, conversion, and validation

If the size of the protected data on your machine allows you to fit in backup as well as additional data processing tasks in your backup window, configure these options in the protection plan itself.

If your data size is too large and the backup barely fits inside your backup window, create separate plans that schedule replication and validation tasks during off-peak hours, like over the weekend.

Other recommendations

Notifications, alerts and reports

The recommended way to manage your backups' status with minimal effort is to set the following notifications:

- Select the **Daily recap about active alerts** check box in notification settings
- Select a time that is convenient for you to check every day. The default is 10:00 am.
- Clear all other check boxes.

These settings will mean you receive a single email every day, which is easy and quick to check. If everything is OK, you will get an email stating this explicitly. If any problems arose during the previous night's backups, you will get a list of alerts clearly stating the problem.

If you need greater control, set the individual alert notifications for critical alerts to make sure you receive an email as soon as a problem appears on your machine.

Note that regular alert notifications are normally sent as soon as an alert is activated. Each alert on each agent for each plan will generate one email.

File format

Whenever possible, use the default Version 12 backup format.

Active Protection

Note
Active Protection is available for machines running Windows 7 and later, Windows Server 2008 R2 and later. Agent for Windows must be installed on the machine.

We recommend that you enable Active Protection on all machines that are not being throttled by lack of CPU resources.

Active Protection will typically have a few percents CPU overhead during heavy file access on the system.

Storage considerations

NAS

The simplest storage for single machines is a NAS or other network folder that contains backups for all the other machines in the environment.

The only real consideration here is to make sure you have enough space on the storage device itself.

You can estimate this size by using our resource usage calculator. The minimum recommended storage space is the size of all backups for your retention period + the size of one full backup of all machines.

USB or internal disk

Another recommended storage option is to have each machine create backups to an attached USB disk or extra internal backup drive.

Offsite storage

It is vitally important to have at least one offsite copy of your data. We recommend using replication to create a copy of data to our own Acronis Cloud Storage in one of the data centers located in your country.

This is the simplest way to get your data securely offsite, but obviously doesn't work for everyone due to WAN upload bandwidth limitations, compliance reasons, cost concerns, etc.

In this case, we recommend replicating the backups to an external USB disk or tape drive and regularly moving this media offsite to a secure location.

Swapped drives

A common scenario in smaller environments is to back up to external removable devices and swap them around on a regular basis.

This does not yet work out of the box with Acronis Cyber Protect because we store backup metadata with the backups themselves. This has a major advantage of making our backups entirely portable: you can take a backup on a USB, ship it across the world to a completely different location and restore with zero knowledge of the original environment.

However, without a mechanism to properly synchronize this metadata across different removable disks (coming in a future release), a regular protection plan to this type of storage will cause any number of issues with backups and retention.

That said, a method for this scenario is described in our Knowledge base.
This is more of a workaround and is by no means an ideal solution, but it is the best way to support this swapped drives until we add support out of the box.

Tape devices

Acronis is committed to continuing and expanded support for tape devices.

For a list of tested and supported tape devices, see the Tape hardware compatibility list.

To check the compatibility of your own tape devices, use the Tape compatibility tool.

If the tool finds a problem, please contact Acronis Support to get this escalated to the development and resolved.

An agent can create backups directly to tape. If you have a single or isolated machine and need to create tape backups, attach the drive directly to the machine that has the agent installed.

Tape management database

Information about all tape devices, tapes and the backup contents is stored in the tape management database located on the machine with the attached tape drive.

The default database path is:

- Windows 7, Server 2008 and later versions of Windows:
  %PROGRAMDATA%\Acronis\BackupAndRecovery\ARSM\Database
- Linux:
  /var/lib/Acronis/BackupAndRecovery/ARSM/Database

The database size depends on the number of backups stored on tapes and equals approximately 10 MB per hundred backups. This usually isn't a problem for a few machines even for long retention periods.

However, please make sure you have enough space for this database on your system. If you are unsure, please change the path before starting any backups to tape.

To relocate the database in Windows

1. Stop the **Removable Storage Management** service.
2. Move all files from the default location to the new location.
3. Find the registry key **HKEY_LOCAL_MACHINE\SOFTWARE\Acronis\ARSM\Settings**.
4. Specify the new location path in the registry value `ArsmDmlDbProtocol`. The string may contain up to 32765 characters.
5. Start the **Removable Storage Management** service.

To relocate the database in Linux

1. Stop the **acronis_rsm** service.
2. Move all files from the default location to the new location.
3. Open the configuration file **/etc/Acronis/ARSM.config** in a text editor.
4. Locate the line `<value name="ArsmDmlDbProtocol" type="TString">`.
5. Change the path under this line.
6. Save the file.
7. Start the **acronis_rsm** service.

Warning!
Do not delete the tape database! This will result in rescanning all tapes to make the backups there usable again. This is a very long operation prone to errors.

Do not enable file recovery from disk backups

This option is disabled by default. Enabling it in your tape management protection plan options will add the ability to restore individual files from image backups stored on tape.

Note that this functionality comes at a steep storage space cost. If this functionality is enabled, at each backup the software creates supplementary files on a hard disk of the machine where the tape device is attached. File recovery from disk backups is possible as long as these supplementary files are intact. The files are deleted automatically when the tape storing the respective backups is erased, removed, or overwritten.

These supplementary files are located:

- In Windows 7 and later versions of Windows:
  %PROGRAMDATA%\Acronis\BackupAndRecovery\TapeLocation
- In Linux:
  /var/lib/Acronis/BackupAndRecovery/TapeLocation

The space occupied by these supplementary files depends on the number of files in the respective backup. For a full backup of a disk containing approximately 20,000 files (the typical workstation disk backup), the supplementary files occupy around 150 MB. A single full backup of a server containing 250,000 files may produce around 700 MB of supplementary files.

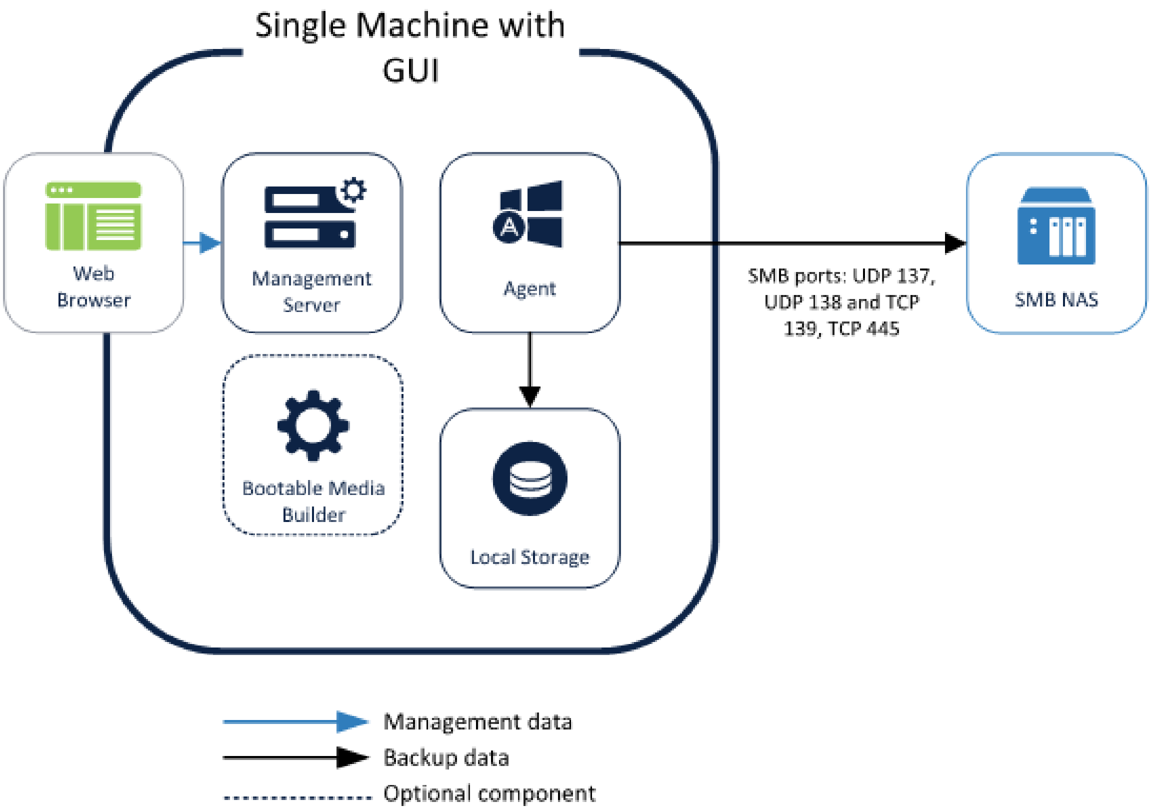
Even in small environments the size of such files will quickly grow to dozens of gigabytes.

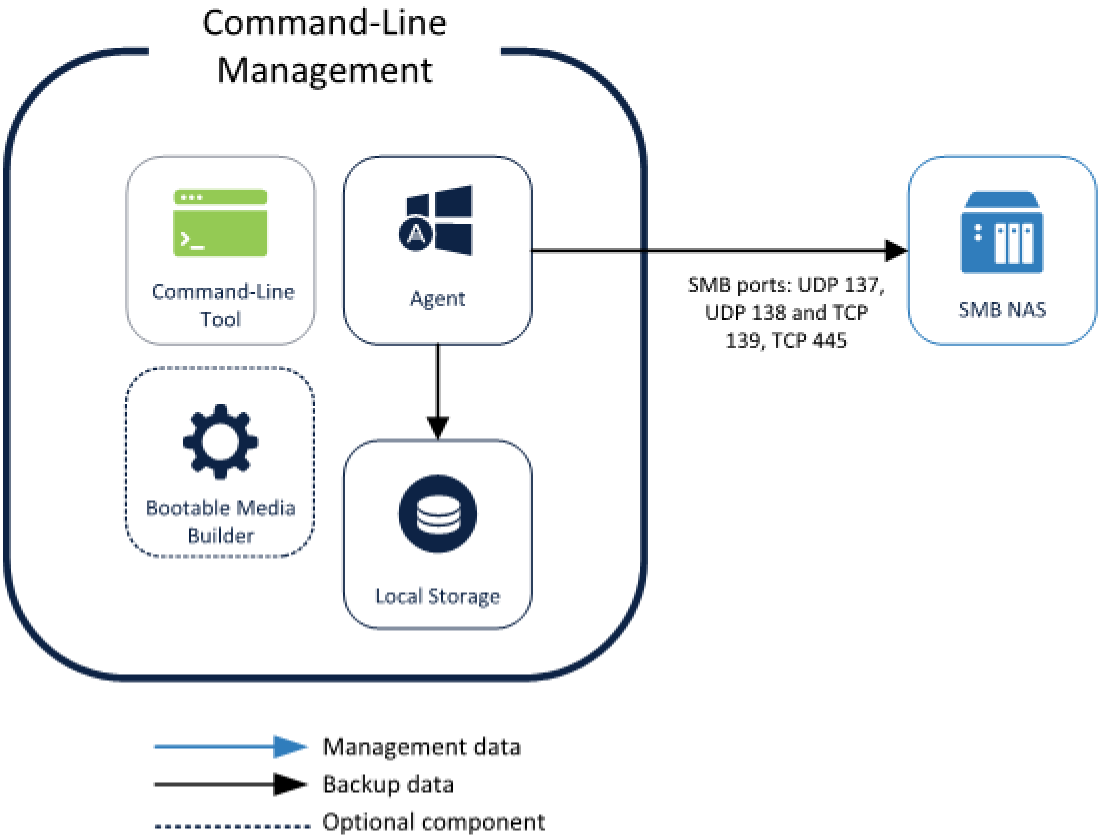
The recommendation is to disable this option unless you absolutely need it and if this is the case, make sure that the Storage Node is sized keeping these supplementary files in mind.

Network diagrams and ports

See the full network diagram in Appendix B.

Below are the network diagrams for single and isolated machines.




Command-Line Management
Command-Line Tool
Agent
SMB ports: UDP 137, UDP 138 and TCP 139, TCP 445
SMB NAS
Bootable Media Builder
Local Storage
Management data
Backup data
Optional component

Small environment

Environment description

Small environments consist of either:

- 2-10 machines in a single network with no dedicated backup server hardware
- 1 Hypervisor or cluster

The key for a successful deployment on this type of environment is to select a single machine to act as your UI and backup server, with all the other machines managed remotely from this single point through the Web console. The backup server would typically be a more powerful physical or virtual machine. This will void the need to install all components on every machine and drastically lower the administrative overhead of managing the environment.

A server operating system is not required for the backup server, even if you want to protect Windows or Linux servers.

Preparing for deployment

This section covers the requirements and recommendations for Acronis Cyber Protect deployment in small environments.

Recommended software requirements for small environments

The list below contains the operating systems to use for installing the Management Server in a small environment. We recommend using a standard Windows operating system, either Windows Server or standard desktop version with no preference between the two ones.

Windows

- Windows 7 – all editions (x86, x64)

  Note
  To use Acronis Cyber Protect with Windows 7, you must install the following updates from Microsoft:
  - Windows 7 Extended Security Updates (ESU)
  - KB4474419
  - KB4490628

  For more information on the required updates, refer to this knowledge base article.

- Windows Server 2008 R2 – Standard, Enterprise, Datacenter, and Foundation editions
- Windows Home Server 2011
- Windows MultiPoint Server 2010/2011/2012
- Windows Small Business Server 2011 – all editions

- Windows 8/8.1 – all editions (x86, x64), except for the Windows RT editions
- Windows Server 2012/2012 R2 – all editions
- Windows Storage Server 2008 R2/2012/2012 R2/2016
- Windows 10 – Home, Pro, Education, Enterprise, IoT Enterprise, and LTSC (formerly LTSB) editions
- Windows Server 2016 – all installation options, except for Nano Server
- Windows Server 2019 – all installation options, except for Nano Server
- Windows 11 – all editions
- Windows Server 2022 – all installation options, except for Nano Server

Hardware requirements and sizing

Although hardware requirements for centralized management grow with the size of your environment, this is negligible at the scale of 10-20 protected devices.

You can find the minimum hardware requirements in the User Guide.

More detailed recommendations on the hardware required to run your backup infrastructure can be found by using our Acronis resource usage calculator.

Deployment type

Acronis Cyber Protect Management Server can be deployed as a physical server, a virtual machine, a Acronis Cyber Protect appliance and finally as a cloud platform to manage your on-premises backup infrastructure.

Depending on the configuration of your environment, please find the recommendations on selecting the deployment type you wish to use.

Purely physical environment

If your environment is made up of purely physical machines, like a couple servers and their attendant workstations, we recommend doing one of the following.

- Dedicate one of these machines in your environment to act as the backup server. Even though our Management Server is optimized for light resource usage, don’t choose the busier production server to act as the backup server. Any machine with a constant network connection and adequate hardware is going to be good enough.
  Make sure that the machine acting as the backup server is not a mobile device that will often leave the network and give it a constant fixed IP address.
- Choose the Cloud deployment model and use the same Management Server, but deployed in Acronis data centers worldwide instead of installing your own instance. Your machines will connect to this cloud Management Server through the WAN.

Note that some advanced features of Acronis Cyber Protect are not yet available with the cloud deployment. They will be propagated to the cloud deployments in a future release.

Purely virtual environment

If you are creating backups of a single hypervisor (or single cluster), we recommend deploying Acronis Cyber Protect as an Acronis Cyber Protect appliance. You can find more information in the User Guide.

Hybrid physical/virtual environment

In this case, the following deployment types are equally valid:

- Install on one of your physical machines.
- Deploy as Acronis Cyber Protect appliance.
- Choose Cloud Deployment.

The choice in this case depends on what is available in your environment.

For example, if your Hypervisor is under constant overload and you have a free physical machine laying around, option 1 would be the best choice.

Conversely, if you have very limited space and powerful Hypervisor, go with option 2.

Cloud deployment is the best choice if you don’t require the advanced features mentioned above.

Components and installation

Management components

If you decide to deploy on a physical machine use the following recommendations to select which components should be installed on the server you chose for the task protection management. Since this will typically not be a dedicated machine in a small environment, the recommendations below are meant to emphasize minimum resource usage over small conveniences.

The following components are recommended:

- **Management Server** is required
- **Bootable Media Builder** has to be installed on at least one machine in your environment and having it next to the Management Server is a good choice

In most cases, the components below are not only not required, they are usually not recommended:

- **Components for Remote Installation** (Windows only)
  This component will allow you to push install Windows agents remotely from inside the GUI of the product. This component requires 2GB+ of free space on your system volume. Install only if you have enough space on the system volume of the Management Sever machine and you would like the added convenience of installing agents remotely
- **Acronis Storage Node**
  This component is only required if you plan to create backups of all your machines to a singe tape

drive. In all other cases, do not install this component.

The following components **should not be installed** in small environments:

- **Catalog Service**
  The catalog service is used exclusively for search inside backups. For example, this is incredibly useful to find specific files at the request of users. Full text search for the content of the documents inside the backup is coming in a future update of Acronis Cyber Protect.

Protection agents

Protection agents need to be installed on each part of the environment you wish to protect.
For instructions on how to install each agent type, please refer to the User Guide.

Physical machines

We recommend installing the agent directly inside the operating system that runs on a physical machine.

Virtual machine environments

This usually means installing one or more agents that communicate directly with the Hypervisor running these machines.

We recommend the following:

Hyper-V environments

Install the Agent for Hyper-V on each Hyper-V host you are running in your infrastructure. Even if the hosts are connected in a cluster, the agent needs to be installed on each host.

Note
If you are using SMB3 shares to store your virtual machines, do not forget to enable the **VSS for SMB File Shares** Windows feature. Your backups will fail without it.

Note
Refer here for more details: https://blogs.technet.microsoft.com/clausjor/2012/06/14/vss-for-smb-file-shares/

VMware vSphere environments

You can deploy one or more Virtual Appliances directly as a virtual machine and/or install an Agent for VMware (Windows). The Virtual Appliance is an instance of Acronis Linux (a custom light-weight Linux distribution created by Acronis) that is running a standard Agent for VMware.

- The standard recommendation is to install a Virtual Appliance on each ESXi host in your virtual environment.
- Installing on a physical machine running Windows is recommended for an offloaded or LAN-free backups.

- Offloaded backup
  - Use if your production ESXi hosts are so heavily loaded that running the virtual appliances is not desirable.
- LAN-free backup
  - If your ESXi uses a SAN attached storage, install the agent on a machine connected to the same SAN. The agent will back up the virtual machines directly from the storage rather than via the ESXi host and LAN. For detailed instructions, see LAN-free backup in the User Guide.

Note that you can install an agent directly inside a specific virtual machine. This will not require an extra license.

This is applicable for scenarios where agentless backup of virtual machines is not supported, such as

- Virtual disk configurations unsupported by snapshots, like raw disks;
- Hypervisors with unsupported agentless backup, such as Xen or RHEV.

Agent for VMware/Hyper-V sizing

Agents for VMware/Hyper-V (whether as a virtual appliance or installed on Windows) are the only agent whose requirements scale with the environment size. The typical minimum recommendation is as follows:

RAM

- 1 GB additional free RAM for the agent if your hypervisor host has 16 GB or less total memory
- 2 GB additional free RAM for the agent if your hypervisor host has up to 64 GB and/or you are backing up 2-4 machines in parallel
- 4 GB additional free RAM for hosts with 64+ of RAM and 4-10 parallel machine backup

CPU

- 2 CPU threads is always recommended
- 2 cores (4 threads) if backing up 5 virtual machines simultaneously
- 4 cores (8 threads) if backing up 10 virtual machines simultaneously

DNS considerations

Proper configuration of Domain Name System (DNS) is critical for virtual backups and is the most common source of various errors and problems. The host names need to be properly resolved between multiple Acronis and VMware components, across multiple physical/virtual networks.

The VMware agent needs to be able to resolve:

- Management Server host name
- Each ESX(i) host name
- vCenter host name

Moreover, each component above has to be able to resolve the names among each other. When the name resolution is not functioning correctly, you will see different categories of errors, from deployment problems to backup errors.

To avoid these errors, follow our recommendations:

When you add a vCenter server into Acronis solution, our product will attempt to deploy a Virtual Appliance on each host running in your vSphere environment. For more details, refer to the User Guide.

For this auto-deployment to work, it is critical for the domain name resolution to work between the Cyber Protect Management Server and the guest operating systems of the virtual machines that run inside your ESX(i) hosts. This is required to ensure that Acronis Agent for VMware (Virtual Appliance) after deployment with configured DNS server is capable for connecting to Cyber Protect Management Server by its host name. To help with this, we added a field that allows selecting how the components connect to the server - via the host name or IP address.

Note
The recommendation is to select the IP address that the agent will use to access the management server instead of using the name.

Once the Appliance for VMware is deployed, check the DNS resolution from the agent to the all the other components:

1. Open a vSphere client and establish connection to an ESX(i) host or vCenter.
2. Navigate to the Virtual Appliance, open the **Console** tab and press Ctrl+Alt+F2 to go into the command-line mode of the Virtual Appliance (press Alt+F1 to return).
3. Ping the ESX host name and vCenter name from inside the Virtual Appliance:
   ```
   ping host name_of_ESX
   ping host name_of_vCenter
   ```
4. If the ping by host name is not successful, you have a DNS resolution problem and the backups of the virtual machines from this agent will not work.

Note
If **Port 25** is blocked, `ping` command will not work correctly. You can try other commands like `nslookup` instead. The actual choice of command is not important as long as it allows you to check connectivity by host name.

You can fix the issue by either properly configuring the network in both the appliance and your virtual environment or by editing the hosts file of each appliance as a workaround.
Use the following procedure to edit the hosts file:

1. Open Virtual Appliance's console by pressing Ctrl+Alt+F2.
2. Open the hosts file with the following command:
   ```
   vi /etc/hosts
   ```
3. Press the i key to enter the edit mode.

4. Write the IP address and the name of the servers that need to be resolved

   ```
   XXX.XXX.XXX.XXX host name
   ```

5. To save changes, press Esc and type

   ```
   :wq
   ```

6. Press Enter.
7. Exit the console by pressing Alt+F1.

Off-host processing

A very important feature of Acronis Cyber Protect Advanced is the ability of Acronis agents to run a number of data-processing tasks besides backup. Each of these tasks can be run on a separate schedule, entirely independent of the backup. The available tasks include:

- Backup replication
- Validation
- Cleanup
- Conversion to VM
- VM replication

Although this functionality is vital for managing the backup data at scale as required by a plan in a way that won’t affect backup windows, it is less important in smaller environments. For example, it allows you to directly replicate your backups directly from one storage end-point to another during the weekends without involving the protection agents themselves.

This functionality is usually not required in smaller environments, where data sizes relative to network bandwidth are usually much smaller, but can be an added convenience, especially if replicating off-site on a weekly or monthly basis.

Recommended installation procedure

You can find detailed installation instructions in the User guide.

When installing on Linux, make sure that the required packages are installed first.

Below are our recommendations for small environments:

1. Register your product in your Acronis account. Detailed instructions are here: https://kb.acronis.com/content/4834.
2. Download the full installation file appropriate to your operating system, Windows or Linux. Files can always be downloaded from your account after they are registered.
3. Install the Cyber Protect Management Server, protection agent, and Bootable Media Builder on the machine chosen as the backup server.
4. Configure your storage locations.
5. Start deploying backup agents.
   a. You can push install from the product if **Components for Remote Installation** are installed.

   b. Otherwise, launch the installation file on each machine that requires protection.
      Note that Linux and Mac agents must be installed manually on each machine you wish to protect.

6. Configure and apply your protection plans.
7. **[Optional]** Configure off-host data processing plans to replicate and validate backups on a weekly/monthly basis.

Protection plan recommendations

What to back up

You will typically want to back up entire machines using a selection of exclusion rules to remove unwanted data from inside the backup.

You can exclude volumes, specific files or extensions. For example, exclude all .avi files from backup of personal notebooks and desktops. Exclusions and other backup options are based on a protection plan, so if different machines require different exclusions, create more than one plan.

Different backup sources will also require the creation of different protection plans, at least one for each type of source.

For example, if you are tight on storage space you can create one full machine protection plan applied to your production server and a second plan applied to personal desktops that creates backups of the user older on each machine by selecting the **[Alluserprofiles]** policy selection rule.

Where to back up

Small environments typically have two main storage options:

- You can store all the backups on the agent itself.
  For example, each machine can backup volume **C:\** to its **D:\** drive or to an external USB drive.
  These scenarios have no specific recommendations.
  This has the benefit of lower network usage, but with a possible administrative overhead cost (each storage location will have to be accessed one by one).
  This option is recommended if you don’t have a centralized file share or NAS to store backups.
- You can store all backups centrally.
  We recommend a standard NAS sized to fit your backup data at the retention period you require.
  Use the resource usage calculator to estimate the approximate backup size given your environment and retention periods.

Scheduling

Unless the network connection from your protected devices to your backup storage is catastrophically inadequate (e.g. you have a 6 TB file server connected to a NAS over a 10 Mb/s link), the backup will not be bottlenecked by your network in a significant manner. This means that the recommended backup schedule will typically depend entirely on the data size of your protected devices and their RPO (recovery point objective) targets. As long as the currently running backup has time to finish before the next one starts, you shouldn't have any problems.

That said, backup does take a non-negligible amount of resources from the machine being protected and this could affect production workloads, especially if they are particularly heavy ones.

Our experience shows that a good basic recommended schedule is to have a daily work day incremental backup running at night after closing hours, with a full backup over the weekend.

It is generally recommended to schedule tasks such as replication and validation separately over the weekend as well, although this isn't very critical for small environments.

How long to keep

Retention periods will often be determined by external policy or compliance rules. You can estimate the size of backups for the retention period by using the resource usage calculator.

If you do not have enough first-tier storage, schedule special replication tasks to move data to a different, cheaper storage solution for long term retention.

For example, you can replicate the backups to Acronis Cloud or make use of tape storage for long term retention.

Replication, conversion, and validation

If you want to minimize the impact of backups on your machines and network, do not set any replication or validation options in your protection plans.

Instead, you can create separate mini-plans that schedule replication and validation tasks off-host during off-peak hours, like over the weekend. It is usually most convenient to specify the agent installed on the Management Server to run these operations

Alternatively, if the different backup + replication + validation and other tasks have enough time to finish during the night without affecting your production, there is nothing wrong with specifying these extra tasks in the protection plan itself. It is, in fact, usually more convenient to manage them this way.

This also applies if each agent is creating a backup into its own direct location. In this case, data-processing tasks like validation have to be scheduled in the protection plan itself.

Other recommendations

Notifications, alerts and reports

You need to keep a close eye on the status of your backups, but small environments don't typically have mission-critical hardware with a dedicated team to start fixing any backup problems ASAP.

Being certain that the daily scheduled backup is working correctly is sufficient in the majority of cases.

The recommended way to manage your backups' status with minimal effort is to set the following notifications:

- Select the **Daily recap about active alerts** check box in notification settings
- Select a time that is convenient for you to check every day. The default is 10:00 am.
- Clear all other check boxes.

These settings will mean you receive a single email every day, which is easy and quick to check. If everything is OK, you will get an email stating this explicitly. If any problems arose during the previous night's backups, you will get a list of alerts clearly stating the problem.

If you need greater control, set the individual alert notifications for critical alerts to make sure you receive an email as soon as a problem appears on your machine.

Note that regular alert notifications are normally sent as soon as an alert is activated. Each alert on each agent for each plan will generate one email.

File format

Whenever possible, use the default Version 12 backup format.

Active Protection

Note
Active Protection is available for machines running Windows 7 and later, Windows Server 2008 R2 and later. Agent for Windows must be installed on the machine.

We recommend that you enable Active Protection on all machines that are not being throttled by lack of CPU resources.

Active Protection will typically have a few percents CPU overhead during heavy file access on the system.

Storage considerations

NAS

The simplest storage for a single machines is a NAS or other network folder that contains backups for all the other machines in the environment.

The only real consideration here is to make sure you have enough space on the storage device itself.

You can estimate this size by using our resource usage calculator. The minimum recommended storage space is the size of all backups for your retention period + the size of one full backup of all machines.

USB or internal disk

Another recommended storage option is to have each machine create backups to an attached USB disk or extra internal backup drive.

Offsite storage

It is vitally important to have at least one offsite copy of your data. We recommend using replication to create a copy of data to our own Acronis Cloud Storage in one of the data centers located in your country.

This is the simplest way to get your data securely offsite, but obviously doesn’t work for everyone due to WAN upload bandwidth limitations, compliance reasons, cost concerns, etc.

In this case, we recommend replicating the backups to an external USB disk or tape drive and regularly moving this media offsite to a secure location.

Deduplication

Do not use deduplication. The hardware overhead is never worth it for the small deduplication gains across a small environment.

Swapped drives

A common scenario in smaller environments is to back up to external removable devices and swap them around on a regular basis.

This does not yet work out of the box with Acronis Cyber Protect because we store backup metadata with the backups themselves. This has a major advantage of making our backups entirely portable: you can take a backup on a USB, ship it across the world to a completely different location and restore with zero knowledge of the original environment.

However, without a mechanism to properly synchronize this metadata across different removable disks (coming in a future release), a regular protection plan to this type of storage will cause any number of issues with backups and retention.

That said, a method for this scenario is described in our Knowledge base.
This is more of a workaround and is by no means an ideal solution, but it is the best way to support this swapped drives until we add support out of the box.

Tape devices

Acronis is committed to continuing and expanded support for tape devices.

For a list of tested and supported tape devices, see the Tape hardware compatibility list.

To check the compatibility of your own tape devices, use the Tape compatibility tool.

If the tool finds a problem, please contact Acronis Support to get this escalated to the development and resolved.

An agent can create backups directly to tape. If you have a single or isolated machine and need to create tape backups, attach the drive directly to the machine that has the agent installed.

Storage Node for tapes

Acronis Storage Node component is required to create centralized backups from multiple machines to one or more tape drives. The tape device needs to be attached to the Storage Node machine.

If you have multiple standalone tape drives or only need a single machine's backups to be stored on tape, we recommend connecting the tape drive directly to the machine(s) being backed up and forgo using the storage node entirely.

Tape management database

Information about all tape devices, tapes and the backup contents is stored in the tape management database located on the machine with the attached tape drive.

The default database path is:

- Windows 7, Server 2008 and later versions of Windows:
  %PROGRAMDATA%\Acronis\BackupAndRecovery\ARSM\Database
- Linux:
  /var/lib/Acronis/BackupAndRecovery/ARSM/Database

The database size depends on the number of backups stored on tapes and equals approximately 10 MB per hundred backups. This usually isn't a problem for a few machines even for long retention periods.

However, please make sure you have enough space for this database on your system. If you are unsure, please change the path before starting any backups to tape.

To relocate the database in Windows

1. Stop the **Removable Storage Management** service.
2. Move all files from the default location to the new location.
3. Find the registry key **HKEY_LOCAL_MACHINE\SOFTWARE\Acronis\ARSM\Settings**.
4. Specify the new location path in the registry value `ArsmDmlDbProtocol`. The string may contain up to 32765 characters.
5. Start the **Removable Storage Management** service.

To relocate the database in Linux

1. Stop the **acronis_rsm** service.
2. Move all files from the default location to the new location.
3. Open the configuration file **/etc/Acronis/ARSM.config** in a text editor.
4. Locate the line `<value name="ArsmDmlDbProtocol" type="TString">`.

5. Change the path under this line.
6. Save the file.
7. Start the **acronis_rsm** service.

Warning!
Do not delete the tape database! This will result in rescanning all tapes to make the backups there usable again. This is a very long operation prone to errors.

Do not enable file recovery from disk backups

This option is disabled by default. Enabling it in your tape management protection plan options will add the ability to restore individual files from image backups stored on tape.

Note that this functionality comes at a steep storage space cost. If this functionality is enabled, at each backup the software creates supplementary files on a hard disk of the machine where the tape device is attached. File recovery from disk backups is possible as long as these supplementary files are intact. The files are deleted automatically when the tape storing the respective backups is erased, removed, or overwritten.

These supplementary files are located:

- In Windows 7 and later versions of Windows:
  %PROGRAMDATA%\Acronis\BackupAndRecovery\TapeLocation
- In Linux:
  /var/lib/Acronis/BackupAndRecovery/TapeLocation

The space occupied by these supplementary files depends on the number of files in the respective backup. For a full backup of a disk containing approximately 20,000 files (the typical workstation disk backup), the supplementary files occupy around 150 MB. A single full backup of a server containing 250,000 files may produce around 700 MB of supplementary files.

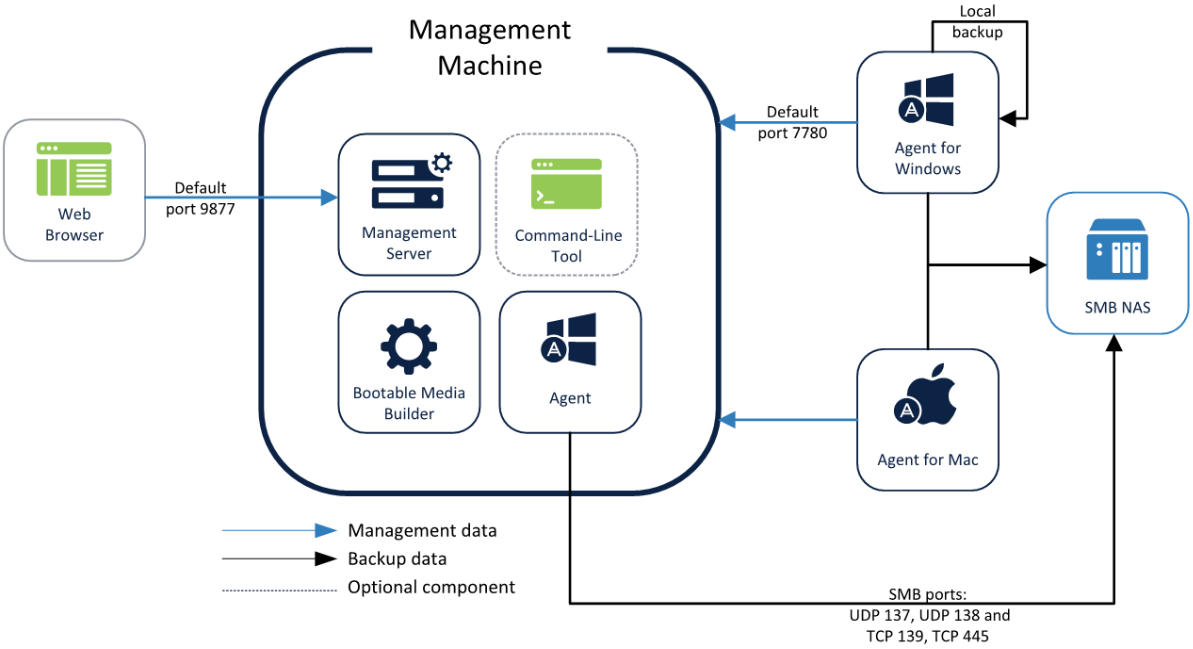
Even in small environments the size of such files will quickly grow to dozens of gigabytes.

The recommendation is to disable this option unless you absolutely need it and if this is the case, make sure that the Storage Node is sized keeping these supplementary files in mind.

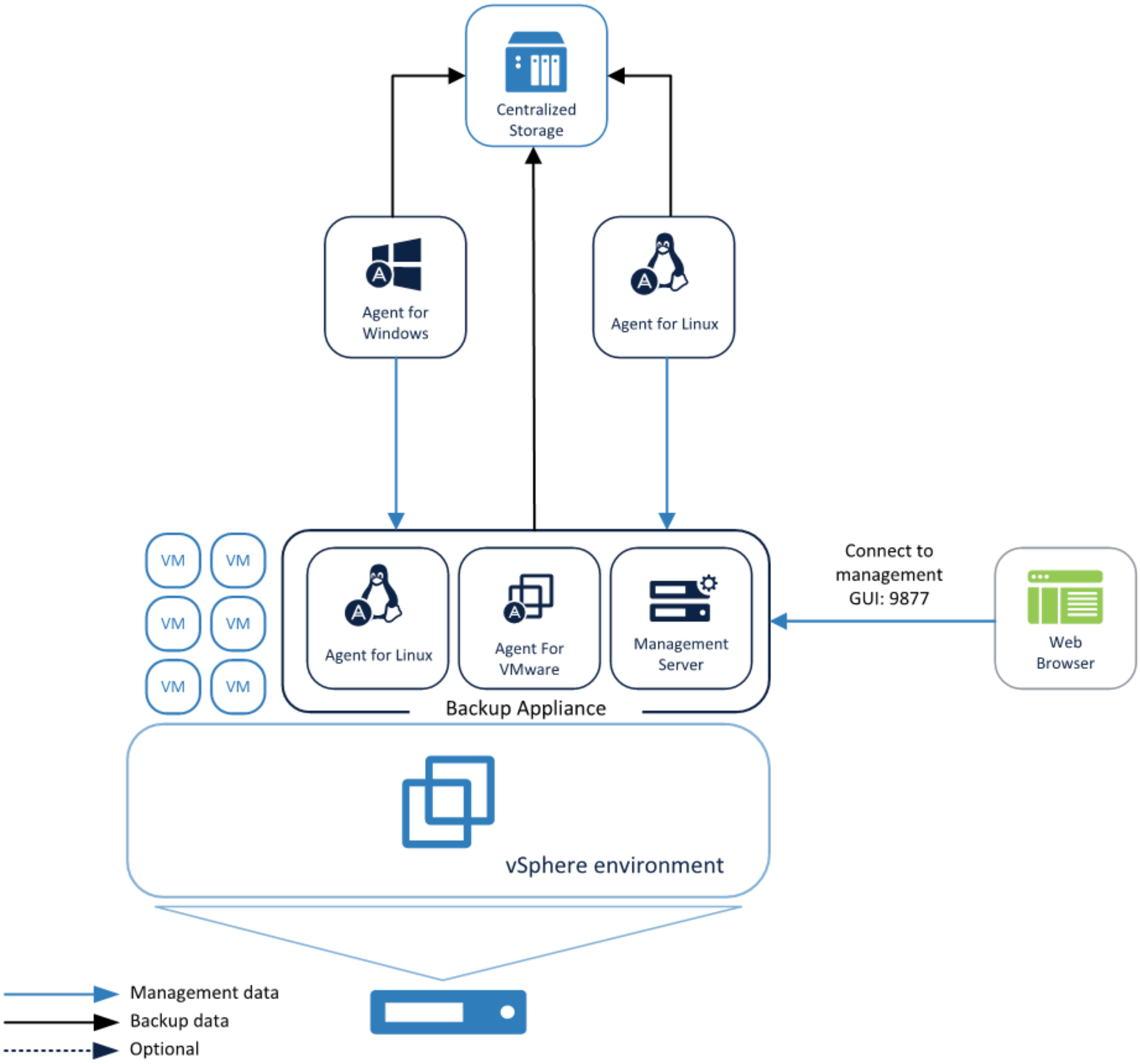
Network diagrams and ports

See the full network diagram in Appendix B.

Below is the network diagram for small environments.



Below is the network diagram if you decide to use Acronis Cyber Protect Appliance.


Centralized Storage
Agent for Windows
Agent for Linux
VM
VM
VM
VM
VM
VM
Agent for Linux
Agent For VMware
Management Server
Backup Appliance
Connect to management GUI: 9877
Web Browser
vSphere environment
Management data
Backup data
Optional

Typical SMB

Environment description

We consider the "typical SMB" to be as follows:

- A couple dozen to a hundred physical servers
  - With 2-3 Linux servers among these
- 1 Hypervisor, usually in a 2-host cluster with up to a couple hundred virtual machines
- A number of production applications that require granular restoration capability

SMB environments also usually have policies that they must adhere to, like: one mandatory off-site copy, replication, validation, etc. Acronis Cyber Protect has a feature called *off-host processing* to simplify these tasks for all SMB environments.

Preparing for deployment

This section covers the requirements and recommendations for Acronis Cyber Protect deployment in SMB environments.

Recommended software requirements for SMB environments

The list below contains supported operating systems for installing the Management Server in an SMB environment.

Note that for predominantly Windows SMB environments we recommend installing the Management Server on Windows Server 2012 R2 or higher although it is possible to use a machine with an older Windows version or with Linux.

Windows

- Windows 7 – all editions (x86, x64)

> **Note**
> To use Acronis Cyber Protect with Windows 7, you must install the following updates from Microsoft:
> - Windows 7 Extended Security Updates (ESU)
> - KB4474419
> - KB4490628
>
> For more information on the required updates, refer to this knowledge base article.

- Windows Server 2008 R2 – Standard, Enterprise, Datacenter, and Foundation editions
- Windows Home Server 2011
- Windows MultiPoint Server 2010/2011/2012
- Windows Small Business Server 2011 – all editions

- Windows 8/8.1 – all editions (x86, x64), except for the Windows RT editions
- Windows Server 2012/2012 R2 – all editions
- Windows Storage Server 2008 R2/2012/2012 R2/2016
- Windows 10 – Home, Pro, Education, Enterprise, IoT Enterprise, and LTSC (formerly LTSB) editions
- Windows Server 2016 – all installation options, except for Nano Server
- Windows Server 2019 – all installation options, except for Nano Server
- Windows 11 – all editions
- Windows Server 2022 – all installation options, except for Nano Server

Although there is no strict requirement to use a Windows Server operating system, this is generally recommended for middle to larger environments due to scalability, security, and stability reasons.

Management Server database

By default, Acronis Management Server uses an SQLite database backend for storing its data in both Windows and Linux environments. This default database choice is largely sufficient for the majority of SMB environments.

However, if you are concerned about the database reliability or have a company policy requirement to use dedicated MS SQL instances, you can select a Microsoft SQL database during the installation. For more information, refer to "MS SQL database recommendations" (p. 59).

When using the Linux management server at these environment sizes, we recommend to use a PostgreSQL database. To configure it, follow the procedure described in KB article https://kb.acronis.com/content/60395.

Note
SQLite might still be installed and used locally for some other services, but will not contain the main product database.

Hardware requirements and sizing

Hardware requirements for the centralized management components scale with the number of devices being managed, especially for environments with over 200 machines.

The Management Server is well optimized and not overly CPU or RAM dependent so any moderately modern server should be fine for an SMB environment. That said, the Management Server is sensitive to I/O throughput of the storage subsystem used by the different databases of the Management Server services. This is due to the fact that simultaneous backups of hundreds of devices generate a lot (hundreds to thousands) of IOPS, which could be a severe bottleneck on a standard HDD.

We recommend that you use high-IOPS disks (SSD) for the Management Server for any environments that contain hundreds of protected devices.

Specific recommendations on the hardware required to run your backup infrastructure can be estimated by using our Acronis resource usage calculator.

Deployment type

Acronis Cyber Protect Management Server can be deployed as a physical server, a virtual machine, an Acronis Cyber Protect appliance and finally as a cloud platform to manage your on-premises backup infrastructure.

Even though IOPS performance of the server storage subsystem is not as critical for SMB environments, it is still an important factor. It is thus generally recommended to use a physical server as the simplest solution in terms of optimized storage subsystem performance.

If your Hypervisor can provide an adequately fast virtual disk subsystem (100+ IOPS), you can also deploy the Management Server on a virtual machine or as an Acronis Cyber Protect appliance.

Acronis Cyber Protect Cloud deployment is the same Acronis Cyber Protect Management Server, but working inside an Acronis data center. Agents connect to this cloud Management Server through the WAN. This deployment type is not recommended as the main scenario for large environments because a number of features used for large environments are available in on-premises deployments only.

Components and installation

Management components

The **Management Server** component must be installed on the server dedicated to the protection management.

In some cases, it is also recommended to install the components below.

- **Scan Service**
  This component performs antimalware scan of backups in a cloud storage, a local or shared folder. Scan Service requires Microsoft SQL Server or PostgreSQL Server database. We recommend that you install this component on a separate machine.
- **Components for Remote Installation** (Windows only)
  This component will allow you to push install Windows agents remotely from inside the GUI of the product. If you plan to install agents using a group policy, this component is not needed.
- **Protection agent**
  This will allow you to protect the Management Server itself.
  Since the Management Server is not strictly necessary for backups to function on the agent, you can skip this step, but you will have to reinstall and redo the entire configuration if you lose the server and don’t have a backup, and this could take a while for large environments.
  Recommendations on self-protecting the Management Server are found in a subsequent section.
    - There is currently no way to import or export the configuration of the management server.
    - There is no built-in way to make a Management Server cluster.
    - Protecting the Management Server will require a license of the type appropriate to the operating system that you are using for the Management Server.

The following components need to be installed, but not necessarily next to the Management Server. They can also be installed on any machine running a licensed agent if that is more convenient:

- **Bootable Media Builder**
- **MS SQL database** (for environments with more than 900 agents)

The following components should be installed on dedicated hardware, but only if they are required by your protection plans and/or storage type.

Note
The resource usage calculator provides recommendations on the installation and number of these components.

- **Acronis Storage Node**
  This component is required for managed backup locations, which are needed if you plan to use deduplication and/or centralized tape storage, or if you need to use the backup catalog. In all other cases, the Storage Node is not required or recommended.
- **Catalog Service**
  The catalog service is used exclusively for search inside backups. For example, this is incredibly useful when you need to find specific files at the request of users.
  If you do not need to index the content of your backup archives, do not install the catalog.

Protection agents

Protection agents need to be installed on each part of the environment you wish to protect.
For instructions on how to install each agent type, please refer to the User Guide.

Physical machines

We recommend installing the agent directly inside the operating system that runs on a physical machine.

Virtual machine environments

This usually means installing one or more agents that communicate directly with the Hypervisor running these machines.

We recommend the following:

Hyper-V environments

Install the Agent for Hyper-V on each Hyper-V host you are running in your infrastructure. Even if the hosts are connected in a cluster, the agent needs to be installed on each host.

Note
If you are using SMB3 shares to store your virtual machines, do not forget to enable the **VSS for SMB File Shares** Windows feature. Your backups will fail without it.

Note
Refer here for more details: https://blogs.technet.microsoft.com/clausjor/2012/06/14/vss-for-smb-file-shares/

VMware vSphere environments

You can deploy one or more virtual appliances directly as a virtual machine and/or install an Agent for VMware (Windows). The virtual appliance is an instance of Acronis Linux (a custom light-weight Linux distribution created by Acronis) that is running a standard Agent for VMware.

- The standard recommendation is to install a Virtual Appliance on each ESXi host in your virtual environment. This is done automatically when you add a vCenter to your Management Server if the DNS is properly configured.
- Installing on a physical machine running Windows is recommended for an offloaded or LAN-free backups.
    - Offloaded backup
      Use if your production ESXi hosts are so heavily loaded that running the virtual appliances is not desirable.
    - LAN-free backup
      If your ESXi uses a SAN attached storage, install the agent on a machine connected to the same SAN. The agent will back up the virtual machines directly from the storage rather than via the ESXi host and LAN. For detailed instructions, see LAN-free backup in the User Guide.

Note that you can install an agent directly inside a specific virtual machine. This will not require an extra license.

This is applicable for scenarios where agentless backup of virtual machines is not supported, such as

- Virtual disk configurations unsupported by snapshots, like raw disks;
- Hypervisors with unsupported agentless backup, such as Xen or RHEV.

Agent for VMware/Hyper-V sizing

Agents for VMware/Hyper-V (whether as a virtual appliance or installed on Windows) are the only agent whose requirements scale with the environment size. The typical minimum recommendation is as follows:

RAM

- 1 GB additional free RAM for the agent if your hypervisor host has 16 GB or less total memory
- 2 GB additional free RAM for the agent if your hypervisor host has up to 64 GB and/or you are backing up 2-4 machines in parallel
- 4 GB additional free RAM for hosts with 64+ of RAM and 4-10 parallel machine backup

CPU

- 2 CPU threads is always recommended
- 2 cores (4 threads) if backing up 5 virtual machines simultaneously
- 4 cores (8 threads) if backing up 10 virtual machines simultaneously

DNS considerations

Proper configuration of Domain Name System (DNS) is critical for virtual backups and is the most common source of various errors and problems. The host names need to be properly resolved between multiple Acronis and VMware components, across multiple physical/virtual networks.

The VMware agent needs to be able to resolve:

- Management Server host name
- Each ESX(i) host name
- vCenter host name

Moreover, each component above has to be able to resolve the names among each other. When the name resolution is not functioning correctly, you will see different categories of errors, from deployment problems to backup errors.

To avoid these errors, follow our recommendations:

When you add a vCenter server into Acronis solution, our product will attempt to deploy a Virtual Appliance on each host running in your vSphere environment. For more details, refer to the User Guide.

For this auto-deployment to work, it is critical for the domain name resolution to work between the Cyber Protect Management Server and the guest operating systems of the virtual machines that run inside your ESX(i) hosts. This is required to ensure that Acronis Agent for VMware (Virtual Appliance) after deployment with configured DNS server is capable for connecting to Cyber Protect Management Server by its host name. To help with this, we added a field that allows selecting how the components connect to the server - via the host name or IP address.

Note
The recommendation is to select the IP address that the agent will use to access the management server instead of using the name.

Once the Appliance for VMware is deployed, check the DNS resolution from the agent to the all the other components:

1. Open a vSphere client and establish connection to an ESX(i) host or vCenter.
2. Navigate to the Virtual Appliance, open the **Console** tab and press Ctrl+Alt+F2 to go into the command-line mode of the Virtual Appliance (press Alt+F1 to return).
3. Ping the ESX host name and vCenter name from inside the Virtual Appliance:

```
ping host name_of_ESX
ping host name_of_vCenter
```

4. If the ping by host name is not successful, you have a DNS resolution problem and the backups of the virtual machines from this agent will not work.

Note
If **Port 25** is blocked, `ping` command will not work correctly. You can try other commands like `nslookup` instead. The actual choice of command is not important as long as it allows you to check connectivity by host name.

You can fix the issue by either properly configuring the network in both the appliance and your virtual environment or by editing the hosts file of each appliance as a workaround.
Use the following procedure to edit the hosts file:

1. Open Virtual Appliance's console by pressing Ctrl+Alt+F2.
2. Open the hosts file with the following command:
   ```
   vi /etc/hosts
   ```
3. Press the i key to enter the edit mode.
4. Write the IP address and the name of the servers that need to be resolved
   ```
   XXX.XXX.XXX.XXX host name
   ```
5. To save changes, press Esc and type
   ```
   :wq
   ```
6. Press Enter.
7. Exit the console by pressing Alt+F1.

Off-host processing

A very important feature of Acronis Cyber Protect Advanced is the ability of Acronis agents to run a number of data-processing tasks besides backup. Each of these tasks can be run on a separate schedule, entirely independent of the backup. The available tasks include:

- Backup replication
- Validation
- Cleanup
- Conversion to VM
- VM replication

This functionality is vital for managing the backup data as required by a plan in a way that won’t affect backup windows. For example, it allows you to install an agent on your backup storage server and validate/cleanup archives without any impact on the network bandwidth and your backup times. You can also replicate your backups directly from one storage end-point to another during the weekends.

Recommended installation procedure

You can find detailed installation instructions in the User guide.

When installing on Linux, make sure that the required packages are installed first.

Below are our recommendations for SMB environments:

1. Register your product in your Acronis account. Detailed instructions are here: https://kb.acronis.com/content/4834.
2. Download the full installation file appropriate to your operating system, Windows or Linux.

   Files can always be downloaded from your account after they are registered.
3. Install the Cyber Protect Management Server, protection agent, Components for Remote Installation and Bootable Media Builder on your backup server
4. Install the Storage Node or catalog if required on the servers tied to your storage infrastructure and register them with your Management Server.
5. Set up your groups.
6. Configure your storage locations.
   - Install a separate agent on or near the storage location (as close as possible in the network). This agent will be used for off-host data processing tasks like clean-up, validation, and replication of the storage.
7. Configure protection plans and apply to groups.
8. Start deploying protection agents.
   a. It is generally recommended to use the Group Policy to deploy large amounts of agents autonomously.
   b. You can also push install from the product.

      Note that Linux and Mac agents must be installed manually on each machine you wish to protect.
   c. Agents can be added to administrative units during installation by specifying the corresponding account.
9. Apply protection plans where not covered by groups.
10. Deploy agents close to your storage locations. These agents will be used for off-host data processing tasks.
11. Create off-host validation, clean-up, replication, conversion plans to manage your data outside backup windows and networks, without affecting resources on protected machines.

Protection plan recommendations

What to back up

You will typically want to back up entire machines using a selection of exclusion rules to remove unwanted data from inside the backup.

You can exclude volumes, specific files or extensions.

For example, exclude all .avi files from protection plans tied to groups that cover personal notebook endpoints.

Where to back up

SMB environments typically have two main storage options:

- You can store all the backups on or close to the endpoint agent itself.
  For example, each machine can backup volume C:\ to its D:\ drive. These scenarios have no specific recommendations. This has the benefit of lower network usage, but with a possible administrative overhead cost (each storage location will have to be accessed one by one).
  This option is recommended if you have a mass-restore requirement, where hundreds or thousands of machines have to be brought back at the same time with minimal impact. See the Restoration recommendations section for more details.
- You can store all backups centrally.
  For large environments, this requires multiple network segments each with its own storage and/or high bandwidth connections to this storage. Please see the Storage considerations section.
  When backups are stored centrally, all data processing tasks like validation and replication should be done by a dedicated agent tied to this storage.

Scheduling

Your network will be the most typical bottleneck for backups: a limited number of backups can run simultaneously in a subnet segment without overloading it.

Thus, the backup schedule has to be balanced between your RPO (recovery point objective) requirements, the total data size you are backing up and the bandwidth available for moving this data. At typical SMB sizes - a couple dozen devices weighing a few terabytes with a schedule of daily incremental backups, there are usually no specific considerations required.

However, if your environment is on the larger side or with a busy network or you cannot otherwise fit the entire environment in a simple backup schema, the recommendation is to split the backup environment into meaningful custom groups. You can find details on creating groups in our documentation.

Each group should contain the number of agents that will allow the backup to finish within the allotted backup window. To help with this task, you can make use of the resource usage calculator.

Note
Other factors can lengthen the backup time over the expected network bandwidth. For example, application metadata collection for application aware backups of virtual machines can take a long time if there is a problem with the source application. You should monitor the first backup of your group to make sure there are no obvious outliers.

The recommended backup schema is **Always incremental**, because this reduces the number of full backups to a minimum (just the first).

Another option is to have the backup stored directly on each protected resource. The scheduling in this case doesn't really require any specific considerations as the backup will not impact the network.

Both methods work equally well and depend more on your restoration scenarios and storage space availability.

How long to keep

Retention periods will often be determined by external policy or compliance rules. You can estimate the size of backups for the retention period by using the resource usage calculator.

If you do not have enough first-tier storage, schedule special replication tasks to move data to a different, cheaper storage solution for long term retention.
For example, you can replicate the backups to Acronis Cloud or make use of tape storage.

If you are using a very large centralized storage for backups, it is strongly recommended to turn off retention rules in the protection plan. Set the backup itself to **keep backups indefinitely**. This is because any cleanup tasks that you specify in the protection plan itself will be executed by each protection agent after the backup is finished, which will cause extra extra load on the agents and the network when thousands of agents are trying to run a cleanup.

Instead, install a separate agent on the storage itself (or as close as possible) and create special **cleanup plans**. These will be executed by the single agent on their own schedules causing minimal to no network load.

Replication, conversion, and validation

Similar to the cleanup procedure, do not set any replication or validation options in the protection plan that target a centralized storage.

Instead, always create separate mini-plans that schedule replication and validation tasks off-host during off-peak hours.

The agent that does these off-host operations should be installed as close to the storage as possible, with maximum available bandwidth, preferably on the storage device itself.

Note
This does not apply if each agent is creating a backup into its own direct location. In this case, data-processing tasks like validation have to be scheduled in the protection plan itself.

Number of resources per protection plan

The typical practical limitation on the number of resources covered by a single plan is tied to the network bandwidth, but this is not always the case. Certain backup workflows do not involve moving large amounts of backup data through the local network. Examples include:

- Office 365 mailbox backups
- Storing the backups locally on each resource

In these cases, the number of simultaneous backups running at once is still limited by the ability of the Management Server to properly update and track all these activities.

The recommended maximum number of resources (including mailboxes, virtual machines and physical agents) to include in a single protection plan is 500 for an optimal performance.

Other recommendations

Notifications, alerts and reports

In order to reduce the administrative overhead of dealing with this flow of information, consider the following tips:

- Disable unnecessary alert types on your environment.
  For example, if you are protecting notebooks or other mobile endpoints, the **Backup status is unknown** alert is generally not very useful, because this alert type is constantly triggering when employees leave the network and the Management Server loses control of the agent.
  You can also lower or raise the priority of certain alerts.

  Note
  These changes work on the level of the entire Management Server and cannot yet be customized per user or organizational unit.

- Notifications are normally sent as soon as an alert is activated.
  Each alert context is specific for the agent and plan for which it was activated on. This means that if the same plan fails on two agents or the same agent has two different plan failures, two alerts will be generated and two letters sent. When scaled to dozens of agents, common failures (like network outage) will mean dozens of letters about the same issue.
  For this reason, we recommend setting per-alert notifications only on the most critical alert types for the plans covering critical infrastructure that require immediate action. For less critical machines, make use of daily scheduled alert reports and the reporting functionality to get a daily snapshot of their status.
- Use the **No successful backups for a specified number of consecutive days** alert in the protection plan options.
  This alert will activate only if a device hasn’t had a successful backup after a defined number of days. This is a useful way to ignore single day backup errors on machines where a single missed backup is not critical.

Error handling retries

When a recoverable error occurs, the program re-attempts to perform the unsuccessful operation (for example, the network becomes unavailable). The default for these attempts is 30 re-attempts with 30 second intervals (15 minutes). This is not critical for a smaller backup jobs, but can significantly impact backup windows if you are running backups of large machine groups in parallel. You can lower this value to 10 re-attempts with 30 second intervals.

File format

Whenever possible, use the default Version 12 backup format.

Active Protection

Note

Active Protection is available for machines running Windows 7 and later, Windows Server 2008 R2 and later. Agent for Windows must be installed on the machine.

We recommend that you enable Active Protection on all machines that are not being throttled by lack of CPU resources.
Active Protection will typically have a few percents CPU overhead during heavy file access on the system.

Management Server self-protection

Make sure that the Management Server itself is also protected by a protection plan.

It is not strictly required to protect it because you can run a disaster recovery your entire environment using just our bootable media in isolation, but not having a backup of the Management Server will mean you have to reinstall the server, re-add each agent and redo the entire configuration after having restored your protected devices.

Having a backup of the Management Server will also enable such options as running it as a virtual machine or converting it into a virtual standby in order to accelerate recovery procedures (see Recovery recommendations section).

Storage considerations

As mentioned previously, an important consideration is the bandwidth of your centralized storage in regards to the number of concurrent backups saving data to this storage.

The resource usage calculator helps by providing an estimate on how many storage segments you will need to do a full backup of all your machines at the specified bandwidth and backup windows.

Deduplication

Deduplication is always at source in Acronis Cyber Protect, meaning that hash calculation is done by the agent and data already contained inside the backup is not resent over the network. This is a great way to reduce both storage needs and network bandwidth, especially if you are creating backups of similar machines.

Note that deduplication is a complex process that comes at the cost of using a moderately powerful storage server and lack of certain features, namely the lack of version 12 backup format support.

If you plan to use deduplication, definitely read more on deduplication technology and the best practices when using it in the Deduplication section of the User guide.

Deduplication makes the most sense when you are creating backups of many machines with a sizable percentage of identical data or when you need to store backups on a storage located on a WAN or other narrow bandwidth connection.

This is rarely the case for SMB environments so the general recommendation for the majority of these cases is to forgo deduplication.

Deduplication and replication

The general recommendation is that replication should always be **to** a deduplicated location and never **from** a deduplicated one.

The reason behind this has to do with the fact that replication in Acronis Cyber Protect is not a simple copy of the archive data and acts more like a re-backup than a copy. This means that when you replicate to a deduplicated location, only the unique data is transferred, exactly as it would be for a backup. This is a major advantage if, for example, you are backing up locally and then replicating to an offsite deduplicated location.

This also means that data replicated from a deduplicated location is reconstituted during replication, meaning that the resulting file is no longer deduplicated and can be used in isolation from the deduplication service on the Storage Node.

This data reconstitution process causes a lot of overhead for the replication operation and it will take longer than if you were replicating from a non-deduplicated location. This will cause problems at scale, especially if the destination is a tape library and thus sensitive to delay.

Tape devices

Acronis is committed to continuing and expanded support for tape devices.

For a list of tested and supported tape devices, see the Tape hardware compatibility list.

To check the compatibility of your own tape devices, use the Tape compatibility tool.

If the tool finds a problem, please contact Acronis Support to get this escalated to the development and resolved.

An agent can create backups directly to tape. If you have a single or isolated machine and need to create tape backups, attach the drive directly to the machine that has the agent installed.

Storage Node for tapes

The Acronis Storage Node is required to create centralized backups from multiple agents to one or more tape drives. The tape device needs to be attached to the Storage Node.

If you plan to use both tapes and deduplication, the recommendation is to install a separate storage node for each storage as there is no practical limit to the number of storage nodes you can manage with one Management Server.

Tape management database

Information about all tape devices, tapes and the backup contents is stored in the tape management database located on the machine with the attached tape drive.

The default database path is:

- Windows 7, Server 2008 and later versions of Windows:
  %PROGRAMDATA%\Acronis\BackupAndRecovery\ARSM\Database
- Linux:
  /var/lib/Acronis/BackupAndRecovery/ARSM/Database

The database size depends on the number of backups stored on tapes and equals approximately 10 MB per hundred backups. This usually isn’t a problem for a few machines even for long retention periods.

However, please make sure you have enough space for this database on your system. If you are unsure, please change the path before starting any backups to tape.

To relocate the database in Windows

1. Stop the **Removable Storage Management** service.
2. Move all files from the default location to the new location.
3. Find the registry key **HKEY_LOCAL_MACHINE\SOFTWARE\Acronis\ARSM\Settings**.
4. Specify the new location path in the registry value `ArsmDmlDbProtocol`. The string may contain up to 32765 characters.
5. Start the **Removable Storage Management** service.

To relocate the database in Linux

1. Stop the **acronis_rsm** service.
2. Move all files from the default location to the new location.
3. Open the configuration file **/etc/Acronis/ARSM.config** in a text editor.
4. Locate the line `<value name="ArsmDmlDbProtocol" type="TString">`.
5. Change the path under this line.
6. Save the file.
7. Start the **acronis_rsm** service.

Warning!
Do not delete the tape database! This will result in rescanning all tapes to make the backups there usable again. This is a very long operation prone to errors.

Do not enable file recovery from disk backups

This option is disabled by default. Enabling it in your tape management protection plan options will add the ability to restore individual files from image backups stored on tape.

Note that this functionality comes at a steep storage space cost. If this functionality is enabled, at each backup the software creates supplementary files on a hard disk of the machine where the tape device is attached. File recovery from disk backups is possible as long as these supplementary files are intact. The files are deleted automatically when the tape storing the respective backups is erased, removed, or overwritten.

These supplementary files are located:

- In Windows 7 and later versions of Windows: **%PROGRAMDATA%\Acronis\BackupAndRecovery\TapeLocation**
- In Linux: **/var/lib/Acronis/BackupAndRecovery/TapeLocation**

The space occupied by these supplementary files depends on the number of files in the respective backup. For a full backup of a disk containing approximately 20,000 files (the typical workstation disk backup), the supplementary files occupy around 150 MB. A single full backup of a server containing 250,000 files may produce around 700 MB of supplementary files.

Even in small environments the size of such files will quickly grow to dozens of gigabytes.

The recommendation is to disable this option unless you absolutely need it and if this is the case, make sure that the Storage Node is sized keeping these supplementary files in mind.

Tape sets

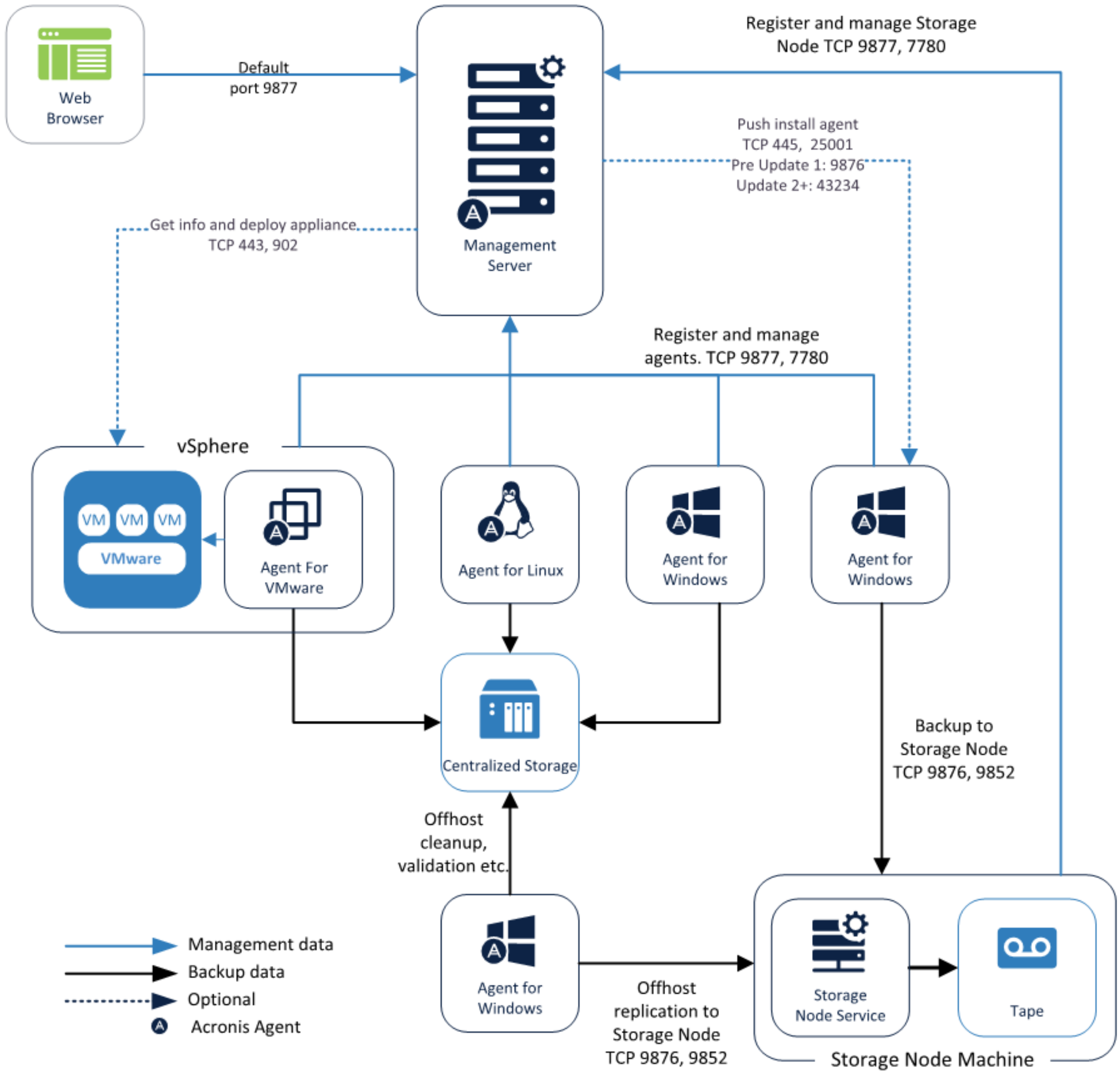
Acronis Cyber Protect supports the creation of tape sets, which give you greater flexibility in managing which exact devices create backups to which tapes and the conditions under which this happens. For example, if you want to use a distinct tape every single day of the work week and then another set of tapes over the weekend.

Refer to the knowledge base article on tape sets at https://kb.acronis.com/content/59315.

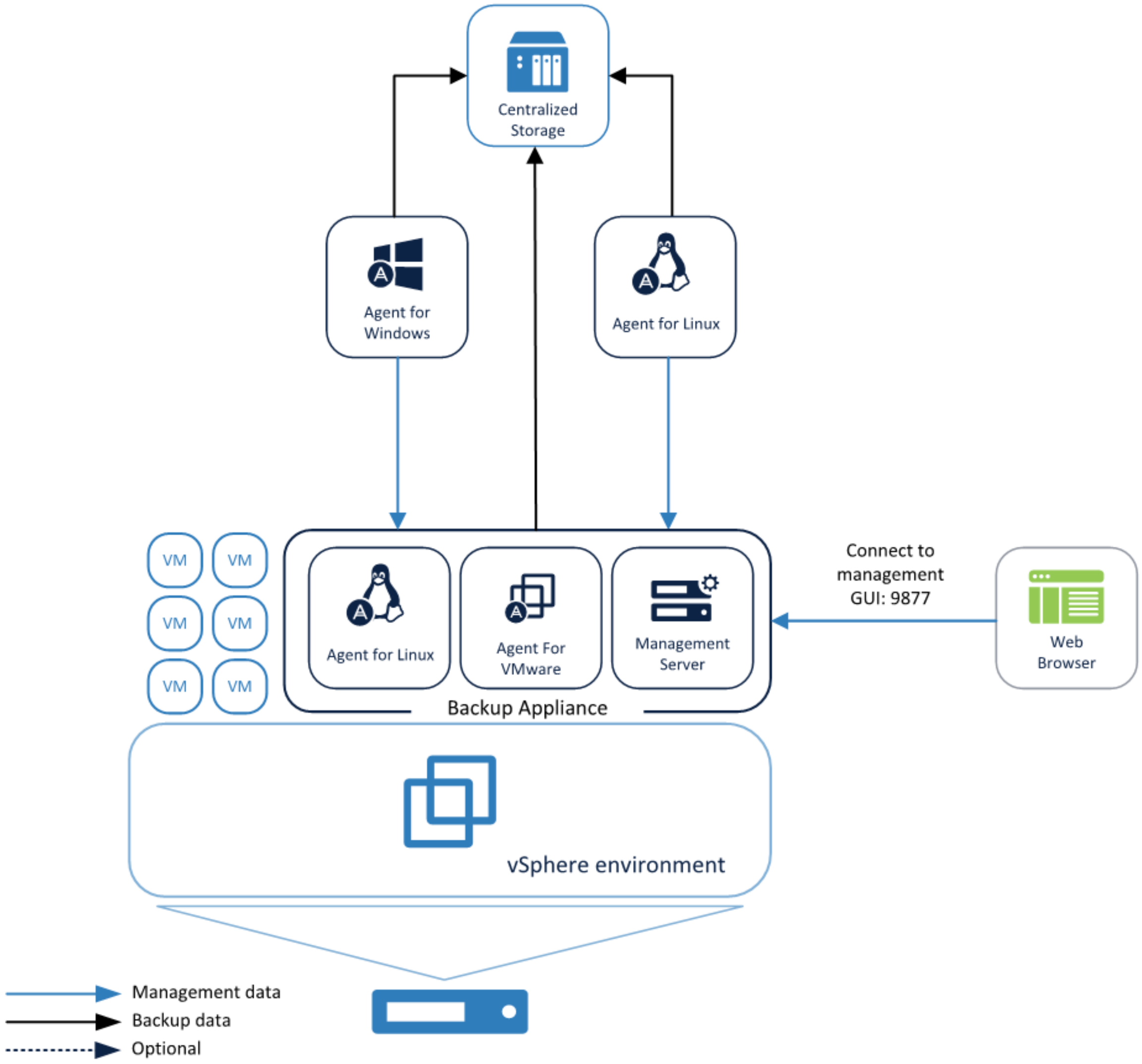
Network diagrams and ports

See the full network diagram in Appendix B.

Below is the network diagram for typical SMB environments.


Web Browser
Default port 9877
Management Server
Register and manage Storage Node TCP 9877, 7780
Push install agent TCP 445, 25001 Pre Update 1: 9876 Update 2+: 43234
Get info and deploy appliance TCP 443, 902
Register and manage agents. TCP 9877, 7780
vSphere
VM
VM
VM
VMware
Agent For VMware
Agent for Linux
Agent for Windows
Agent for Windows
Centralized Storage
Backup to Storage Node TCP 9876, 9852
Offhost cleanup, validation etc.
Agent for Windows
Offhost replication to Storage Node TCP 9876, 9852
Storage Node Service
Tape
Storage Node Machine
Management data
Backup data
Optional
Acronis Agent

Below is the network diagram if you decide to use Acronis Cyber Protect Appliance.


Centralized Storage
Agent for Windows
Agent for Linux
VM
VM
VM
VM
VM
VM
Agent for Linux
Agent For VMware
Management Server
Backup Appliance
Connect to management GUI: 9877
Web Browser
vSphere environment
Management data
Backup data
Optional

Large environment

Environment description

Such environments are made up of hundreds of machines that need to be backed up with a dedicated infrastructure for backup.

The key takeaway for these environments is that a simultaneous backup of hundreds of machines will overload any network and slow it to a crawl. In order to avoid this, the management components have to be installed on proper dedicated hardware and the protection plans must be carefully managed in terms of backup schedules.

Starting with Update 4, Acronis Cyber Protect can support up to 8000 resources on a single properly configured (see below) management server as described in the current chapter.

Preparing for deployment

This section covers the requirements and recommendations for Acronis Cyber Protect deployment in large environments.

Recommended software requirements for large environments

The list below contains supported operating systems for installing the Management Server in a large environment.

For predominantly Windows environments we recommend installing the Management Server on Windows Server 2012 R2 or higher although it is possible to use a machine with an older Windows version or with Linux.

Also note, that it's not possible to create administrative units under Linux.

Windows

- Windows 7 – all editions (x86, x64)

Note
To use Acronis Cyber Protect with Windows 7, you must install the following updates from Microsoft:

- Windows 7 Extended Security Updates (ESU)
- KB4474419
- KB4490628

For more information on the required updates, refer to this knowledge base article.

- Windows Server 2008 R2 – Standard, Enterprise, Datacenter, and Foundation editions
- Windows Home Server 2011
- Windows MultiPoint Server 2010/2011/2012

- Windows Small Business Server 2011 – all editions
- Windows 8/8.1 – all editions (x86, x64), except for the Windows RT editions
- Windows Server 2012/2012 R2 – all editions
- Windows Storage Server 2008 R2/2012/2012 R2/2016
- Windows 10 – Home, Pro, Education, Enterprise, IoT Enterprise, and LTSC (formerly LTSB) editions
- Windows Server 2016 – all installation options, except for Nano Server
- Windows Server 2019 – all installation options, except for Nano Server
- Windows 11 – all editions
- Windows Server 2022 – all installation options, except for Nano Server

Although there is no strict requirement to use a Windows Server operating system, this is generally recommended for large environments due to scalability, security and stability reasons.

Linux

Note

The following Linux distributions and kernel versions have been specifically tested. However, even if your Linux distribution or kernel version is not listed below, it may still work correctly in all required scenarios, due to the specifics of the Linux operating systems.

If you encounter issues while using Acronis Cyber Protect with your combination of Linux distribution and kernel version, contact the Support team for further investigation.

Linux with kernel from 2.6.9 to 5.19 and glibc 2.3.4 or later, including the following x86_64 distributions.

x86 distributions are not supported.

- Red Hat Enterprise Linux 6.x, 7.x, 8.0, 8.1, 8.2, 8.3, 8.4*, 8.5*, 8.6*, 8.7*
- Ubuntu 9.10, 10.04, 10.10, 11.04, 11.10, 12.04, 12.10, 13.04, 13.10, 14.04, 14.10, 15.04, 15.10, 16.04, 16.10, 17.04, 17.10, 18.04, 18.10, 19.04, 19.10, 20.04, 20.10, 21.04, 21.10, 22.04
- Fedora 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31
- SUSE Linux Enterprise Server 10, 11, 12, 15

  Important

  Configurations with Btrfs are not supported for SUSE Linux Enterprise Server 12 and SUSE Linux Enterprise Server 15.

- Debian 4.x, 5.x, 6.x, 7.0, 7.2, 7.4, 7.5, 7.6, 7.7, 8.0, 8.1, 8.2, 8.3, 8.4, 8.5, 8.6, 8.7, 8.8, 8.11, 9.0, 9.1, 9.2, 9.3, 9.4, 9.5, 9.6, 9.7, 9.8, 10.x, 11.x
- CentOS 5.x, 6.x, 7.x, 8.0, 8.1, 8.2, 8.3, 8.4*, 8.5*
- CentOS Stream 8
- Oracle Linux 5.x, 6.x, 7.x, 8.0, 8.1, 8.2, 8.3, 8.4*, 8.5*– both Unbreakable Enterprise Kernel and Red Hat Compatible Kernel
- CloudLinux 5.x, 6.x, 7.x, 8.0, 8.1, 8.2, 8.3, 8.4*, 8.5*

- ClearOS 5.x, 6.x, 7.x, 8.0, 8.1, 8.2, 8.3, 8.4*, 8.5*
- AlmaLinux 8.4*, 8.5*
- Rocky Linux 8.4*
- ALT Linux 7.0

Before installing the product on a system that does not use RPM Package Manager, such as an Ubuntu system, you need to install this manager manually; for example, by running the following command (as the root user): `apt-get install rpm`

If your Linux distribution does not support the D-Bus mechanism (for example, Red Hat Enterprise Linux 6.x or CentOS 6.x) Acronis Cyber Protect will use the default location for storing secure keys because the operating system does not provide D-Bus compatible location.

* Supported only with kernels from 4.18 to 5.19

Management Server database

By default, Acronis Management Server uses an SQLite database backend for storing its data in both Windows and Linux environments.

Note
For large environments, we recommended that you avoid the default SQLite database and use a more robust and secure solution instead.

- For Windows, we recommend Microsoft SQL Server. We do not recommend the SQL Express edition for large environments.
- For Linux, we recommend PostgreSQL. To configure this database, follow the procedure described in https://kb.acronis.com/content/60395.

MS SQL database recommendations

Here are two reference configurations for running about 10 000 protection agents on an MS SQL backend for the database. For best results, use a configuration that meets the recommended requirements.

	Minimum	Recommended
CPU	8	12
RAM	20 GB	32 GB
Disk	150 GB SSD	300 GB SSD
Network	10 MB/s	30 MB/s

Hardware requirements and sizing

The hardware requirements for most peripheral Acronis Cyber Protect components (including protection agents) do not change with scale. No matter how many individual agents are installed, the individual requirements for each agent depend on the data size being backed up on each specific machine regardless of the total number of agents.

Hardware requirements for the centralized management components scale with the number of devices being managed, especially for environments with over 200 machines.

Since the Management Server is not overly CPU or RAM dependent, the key requirement for these larger environments is the I/O throughput of the storage subsystem used by the different databases of the Management Server services. This is because backups in large environments generate a lot (hundreds to thousands) of IOPS, which could be a severe bottleneck on a standard HDD.

We recommend that you use high-IOPS disks for the Management Server of larger environments, such as an SSD.

Here are two reference configurations for the Management Server machine in environments with about 10 000 protection agents.

	Minimum	**Recommended**
CPU	8	16
RAM	20 GB	32 GB
Disk	150 GB SSD	300 GB SSD
Network	10 MB/s	30 MB/s
Simultaneously running protection tasks	No more than 500	

For best results, use a configuration that meets the recommended requirements. On such a configuration, about 500 protection tasks can run simultaneously, with a new batch starting every 15 minutes. Task running time is about 10 minutes.

Specific recommendations on the hardware required to run your backup infrastructure can be estimated by using our Acronis resource usage calculator.

Deployment type

Acronis Cyber Protect Management Server can be deployed as a physical server, a virtual machine, an Acronis Cyber Protect appliance and finally as a cloud platform to manage your on-premises backup infrastructure.

For large environments, it is generally recommended to use a physical server due to the hardware requirements and IOPS load on the disk subsystem.

Acronis Cyber Protect Cloud deployment is the same Acronis Cyber Protect Management Server, but working inside an Acronis data center. Agents connect to this cloud Management Server through the WAN. This deployment type is not recommended as the main scenario for large environments because a number of features used for large environments are available in on-premises deployments only. They will be propagated to the cloud deployments in a future release.

Post-deployment optimization for large environments

Activity retention

Activities are retained for 90 days. On large environments with thousands of machines, the activities log might become too large to be handled effectively, thus making the **Activities** dashboard less responsive.

We recommend lowering the activity retention to 30 days.

To lower the activity retention

1. Open the `task_manager.yaml` file for editing.

   You can find the `task_manager.yaml` file in the following locations:

   - Windows:`%Program Files%\Acronis\TaskManager\`
   - Linux:`/var/lib/Acronis/TaskManager/`

2. In the `database` section, find the settings for the `default` shard space.

   For example:

   ```
   shards:
     - connection-string: sqlite://task-manager.sqlite
       days-to-keep: 90
       space: "default"
       key: "00000000-0000-0000-0000-000000000000"
   ```

3. On the `days-to-keep` line, change the value to 30.

   ```
   days-to-keep: 30
   ```

4. Save your changes, and then restart the Acronis Management Server service.

Storage usage data

Storage usage widgets show data that is updated every five minutes. If you plan to add more than 2000 workloads and if you use local or mounted network storages, we recommend updating this data less frequently – for example, every hour.

You do not need to change this setting if you only use the cloud storage.

To decrease the update frequency for storage usage data

1. Open the `collector.yml` file for editing.

   You can find the `collector.yml` file in the following locations:

   - Windows: `%ProgramData%\Acronis\MonitoringCollector\`
   - Linux: `/var/lib/Acronis/MonitoringCollector/`
2. On the `vaults_collection_interval` line, change the value (the interval in seconds) from 300 to 3600.

   ```
   vaults_collection_interval: 3600
   ```

   Note
   Keep the default values for `activities_collection_interval`, `alerts_collection_interval`, and `flush_interval` because these settings are not related to performance changes that depend on the number of protected workloads.

3. Save your changes, and then restart the Acronis Service Manager service.

Components and installation

Management components

The **Management Server** component must be installed on the server dedicated to the protection management.

In some cases, it is also recommended to install the components below.

- **Scan Service**
  This component performs antimalware scan of backups in a cloud storage, a local or shared folder. Scan Service requires Microsoft SQL Server or PostgreSQL Server database. We recommend that you install this component on a separate machine.
- **Components for Remote Installation** (Windows only)
  This component will allow you to push install Windows agents remotely from inside the GUI of the product. If you plan to install agents using a group policy, this component is not needed.
- **Protection agent**
  This will allow you to protect the Management Server itself.
  Since the Management Server is not strictly necessary for backups to function on the agent, you can skip this step, but you will have to reinstall and redo the entire configuration if you lose the server and don’t have a backup, and this could take a while for large environments.
  Recommendations on self-protecting the Management Server are found in a subsequent section.
  - There is currently no way to import or export the configuration of the management server.
  - There is no built-in way to make a Management Server cluster.
  - Protecting the Management Server will require a license of the type appropriate to the operating system that you are using for the Management Server.

The following components need to be installed, but not necessarily next to the Management Server. They can also be installed on any machine running a licensed agent if that is more convenient:

- **Bootable Media Builder**
- **MS SQL database** (for environments with more than 900 agents)

The following components should be installed on dedicated hardware, but only if they are required by your protection plans and/or storage type.

Note
The resource usage calculator provides recommendations on the installation and number of these components.

- **Acronis Storage Node**
  This component is required for managed backup locations, which are needed if you plan to use deduplication and/or centralized tape storage, or if you need to use the backup catalog. In all other cases, the Storage Node is not required or recommended.
- **Catalog Service**
  The catalog service is used exclusively for search inside backups. For example, this is incredibly useful when you need to find specific files at the request of users.
  If you do not need to index the content of your backup archives, do not install the catalog.

Protection agents

Protection agents need to be installed on each part of the environment you wish to protect.
For instructions on how to install each agent type, please refer to the User Guide.

Physical machines

We recommend installing the agent directly inside the operating system that runs on a physical machine.

Virtual machine environments

This usually means installing one or more agents that communicate directly with the Hypervisor running these machines.

We recommend the following:

Hyper-V environments

Install the Agent for Hyper-V on each Hyper-V host you are running in your infrastructure. Even if the hosts are connected in a cluster, the agent needs to be installed on each host.

Note
If you are using SMB3 shares to store your virtual machines, do not forget to enable the **VSS for SMB File Shares** Windows feature. Your backups will fail without it.

Note
Refer here for more details: https://blogs.technet.microsoft.com/clausjor/2012/06/14/vss-for-smb-file-shares/

VMware vSphere environments

You can deploy one or more Virtual Appliances directly as a virtual machine and/or install an Agent for VMware (Windows). The Virtual Appliance is an instance of Acronis Linux (a custom light-weight Linux distribution created by Acronis) that is running a standard Agent for VMware.

- The standard recommendation is to install a Virtual Appliance on each ESXi host in your virtual environment.
- Installing on a physical machine running Windows is recommended for an offloaded or LAN-free backups.
  - Offloaded backup
    - Use if your production ESXi hosts are so heavily loaded that running the virtual appliances is not desirable.
  - LAN-free backup
    - If your ESXi uses a SAN attached storage, install the agent on a machine connected to the same SAN. The agent will back up the virtual machines directly from the storage rather than via the ESXi host and LAN. For detailed instructions, see LAN-free backup in the User Guide.

Note that you can install an agent directly inside a specific virtual machine. This will not require an extra license.

This is applicable for scenarios where agentless backup of virtual machines is not supported, such as

- Virtual disk configurations unsupported by snapshots, like raw disks;
- Hypervisors with unsupported agentless backup, such as Xen or RHEV.

Agent for VMware/Hyper-V sizing

Agents for VMware/Hyper-V (whether as a virtual appliance or installed on Windows) are the only agent whose requirements scale with the environment size. The typical minimum recommendation is as follows:

RAM

- 1 GB additional free RAM for the agent if your hypervisor host has 16 GB or less total memory
- 2 GB additional free RAM for the agent if your hypervisor host has up to 64 GB and/or you are backing up 2-4 machines in parallel
- 4 GB additional free RAM for hosts with 64+ of RAM and 4-10 parallel machine backup

CPU

- 2 CPU threads is always recommended
- 2 cores (4 threads) if backing up 5 virtual machines simultaneously
- 4 cores (8 threads) if backing up 10 virtual machines simultaneously

DNS considerations

Proper configuration of Domain Name System (DNS) is critical for virtual backups and is the most common source of various errors and problems. The host names need to be properly resolved between multiple Acronis and VMware components, across multiple physical/virtual networks.

The VMware agent needs to be able to resolve:

- Management Server host name
- Each ESX(i) host name
- vCenter host name

Moreover, each component above has to be able to resolve the names among each other. When the name resolution is not functioning correctly, you will see different categories of errors, from deployment problems to backup errors.

To avoid these errors, follow our recommendations:

When you add a vCenter server into Acronis solution, our product will attempt to deploy a Virtual Appliance on each host running in your vSphere environment. For more details, refer to the User Guide.

For this auto-deployment to work, it is critical for the domain name resolution to work between the Cyber Protect Management Server and the guest operating systems of the virtual machines that run inside your ESX(i) hosts. This is required to ensure that Acronis Agent for VMware (Virtual Appliance) after deployment with configured DNS server is capable for connecting to Cyber Protect Management Server by its host name. To help with this, we added a field that allows selecting how the components connect to the server - via the host name or IP address.

Note
The recommendation is to select the IP address that the agent will use to access the management server instead of using the name.

Once the Appliance for VMware is deployed, check the DNS resolution from the agent to the all the other components:

1. Open a vSphere client and establish connection to an ESX(i) host or vCenter.
2. Navigate to the Virtual Appliance, open the **Console** tab and press Ctrl+Alt+F2 to go into the command-line mode of the Virtual Appliance (press Alt+F1 to return).
3. Ping the ESX host name and vCenter name from inside the Virtual Appliance:
   ```
   ping host name_of_ESX
   ping host name_of_vCenter
   ```

4. If the ping by host name is not successful, you have a DNS resolution problem and the backups of the virtual machines from this agent will not work.

Note
If **Port 25** is blocked, `ping` command will not work correctly. You can try other commands like `nslookup` instead. The actual choice of command is not important as long as it allows you to check connectivity by host name.

You can fix the issue by either properly configuring the network in both the appliance and your virtual environment or by editing the hosts file of each appliance as a workaround.
Use the following procedure to edit the hosts file:

1. Open Virtual Appliance's console by pressing Ctrl+Alt+F2.
2. Open the hosts file with the following command:
   ```
   vi /etc/hosts
   ```
3. Press the i key to enter the edit mode.
4. Write the IP address and the name of the servers that need to be resolved
   ```
   XXX.XXX.XXX.XXX host name
   ```
5. To save changes, press Esc and type
   ```
   :wq
   ```
6. Press Enter.
7. Exit the console by pressing Alt+F1.

Off-host processing

A very important feature of Acronis Cyber Protect Advanced is the ability of Acronis agents to run a number of data-processing tasks besides backup. Each of these tasks can be run on a separate schedule, entirely independent of the backup. The available tasks include:

- Backup replication
- Validation
- Cleanup
- Conversion to VM
- VM replication

This functionality is vital for managing the backup data in large environments. For example, it allows you to install an agent on your backup storage server and validate/cleanup archives without any impact on the network bandwidth and your backup times. You can also replicate your backups directly from one storage end-point to another during the weekends.

Recommended installation procedure

You can find detailed installation instructions in the User guide.

When installing on Linux, make sure that the required packages are installed first.

Below are our recommendations for large environments:

1. Register your product in your Acronis account. Detailed instructions are here: https://kb.acronis.com/content/4834.
2. Download the full installation file appropriate to your operating system, Windows or Linux.

   Files can always be downloaded from your account after they are registered.
3. Install the Cyber Protect Management Server, protection agent, Components for Remote Installation and Bootable Media Builder on your backup server
4. Install the Storage Node or catalog if required on the servers tied to your storage infrastructure and register them with your Management Server.
5. Set up your groups, users and units (see below for recommendations).
6. Configure your storage locations.

   Install a separate agent on or near the storage location (as close as possible in the network). This agent will be used for off-host data processing tasks like clean-up, validation and replication of the storage.
7. Configure protection plans and apply to groups.
8. Start deploying protection agents.
   1. It is generally recommended to use the Group Policy to deploy large amounts of agents autonomously.
   2. You can also push install from the product.

      Note that Linux and Mac agents must be installed manually on each machine you wish to protect.
   3. Agents can be added to administrative units during installation by specifying the corresponding account.
9. Apply protection plans where not covered by groups.
10. Deploy agents close to your storage locations. These agents will be used for off-host data processing tasks.
11. Create off-host validation, clean-up, replication, conversion plans to manage your data outside backup windows and networks, without affecting resources on protected machines.

Protection plan recommendations

What to back up

You will typically want to back up entire machines using a selection of exclusion rules to remove unwanted data from inside the backup.

You can exclude volumes, specific files or extensions.

For example, exclude all .avi files from protection plans tied to groups that cover personal notebook endpoints.

Where to back up

Large environments typically have two main storage options:

- You can store all the backups on or close to the endpoint agent itself.
  For example, each machine can backup volume C:\ to its D:\ drive. These scenarios have no specific recommendations. This has the benefit of lower network usage, but with a possible administrative overhead cost (each storage location will have to be accessed one by one).
  This option is recommended if you have a mass-restore requirement, where hundreds or thousands of machines have to be brought back at the same time with minimal impact. See the Restoration recommendations section for more details.
- You can store all backups centrally.
  For large environments, this requires multiple network segments each with its own storage and/or high bandwidth connections to this storage. Please see the Storage considerations section below.
  When backups are stored centrally, all data processing tasks like validation and replication should be done by a dedicated agent tied to this storage.

Scheduling

For large environments, the network will be the most typical bottleneck for backups: a limited number of backups can run simultaneously in a subnet segment without overloading it.

The recommended way to work within this physical limitation is to split the backup environment into meaningful custom groups. You can find details on creating groups in our documentation.

Each group should contain the number of agents that will allow the backup to finish within the allotted backup window. To help with this task, you can make use of the resource usage calculator.

Note
Other factors can lengthen the backup time over the expected network bandwidth. For example, application metadata collection for application aware backups of virtual machines can take a long time if there is a problem with the source application. You should monitor the first backup of your group to make sure there are no obvious outliers.

The recommended backup schema is **Always incremental**, because this reduces the number of full backups to a minimum (just the first).

Another option is to have the backup stored directly on each protected resource. The scheduling in this case doesn’t really require any specific considerations as the backup will not impact the network.

Both methods work equally well and depend more on your restoration scenarios and storage space availability.

How long to keep

Retention periods will often be determined by external policy or compliance rules. You can estimate the size of backups for the retention period by using the resource usage calculator.

If you do not have enough first-tier storage, schedule special replication tasks to move data to a different, cheaper storage solution for long term retention.
For example, you can replicate the backups to Acronis Cloud or make use of the Acronis Storage solution in your own data center.

If you are using a very large centralized storage for backups, it is strongly recommended to turn off retention rules in the protection plan. Set the backup itself to **keep backups indefinitely**.

This is because any cleanup tasks that you specify in the protection plan itself will be executed by each protection agent after the backup is finished, which will cause extra extra load on the agents and the network when thousands of agents are trying to run a cleanup.

Instead, install a separate agent on the storage itself (or as close as possible) and create special **cleanup plans**. These will be executed by the single agent on their own schedules causing minimal to no network load.

Replication, conversion, and validation

Similar to the cleanup procedure, do not set any replication or validation options in the protection plan that target a centralized storage.

Instead, always create separate mini-plans that schedule replication and validation tasks off-host during off-peak hours.

The agent that does these off-host operations should be installed as close to the storage as possible, with maximum available bandwidth, preferably on the storage device itself.

Note
This does not apply if each agent is creating a backup into its own direct location. In this case, data-processing tasks like validation have to be scheduled in the protection plan itself.

Number of resources per protection plan

The typical practical limitation on the number of resources covered by a single plan is tied to the network bandwidth, but this is not always the case. Certain backup workflows do not involve moving large amounts of backup data through the local network. Examples include:

- Office 365 mailbox backups
- Storing the backups locally on each resource

In these cases, the number of simultaneous backups running at once is still limited by the ability of the Management Server to properly update and track all these activities.

The recommended maximum number of resources (including mailboxes, virtual machines and physical agents) to include in a single protection plan is 500 for an optimal performance.

Other recommendations

Notifications, alerts and reports

Even very stable environments tend to have a lot of daily errors to process when the protected devices number in the thousands.

In order to reduce the administrative overhead of dealing with this flow of information, consider the following tips:

- Disable unnecessary alert types on your environment.
  For example, if you are protecting notebooks or other mobile endpoints, the **Backup status is unknown** alert is generally not very useful, because this alert type is constantly triggering when employees leave the network and the Management Server loses control of the agent.
  You can also lower or raise the priority of certain alerts.

  Note
  These changes work on the level of the entire Management Server and cannot yet be customized per user or organizational unit.

- Notifications are normally sent as soon as an alert is activated. Each alert context is specific for the agent and plan for which it was activated on.
  This means that if the same plan fails on two agents or the same agent has two different plan failures, two alerts will be generated and two letters sent. When scaled to dozens of agents, common failures (like network outage) will mean dozens of letters about the same issue.
  For this reason, we recommend setting per-alert notifications only on the most critical alert types for the plans covering critical infrastructure that require immediate action. For less critical machines, make use of daily scheduled alert reports and the reporting functionality to get a daily snapshot of their status.
- Use the **No successful backups for a specified number of consecutive days** alert in the protection plan options.
  This alert will activate only if a device hasn’t had a successful backup after a defined number of days. This is a useful way to ignore single day backup errors on machines where a single missed backup is not critical.

Units

When multiple people are in charge of administrating the backup environment, make sure to divide the environment into organization units as described in the User guide.

Error handling retries

When a recoverable error occurs, the program re-attempts to perform the unsuccessful operation (for example, the network becomes unavailable). The default for these attempts is 30 re-attempts with 30 second intervals (15 minutes). This is not critical for a smaller backup jobs, but can significantly impact backup windows if you are running backups of large machine groups in parallel. You can lower this value to 10 re-attempts with 30 second intervals.

File format

Whenever possible, use the default Version 12 backup format.

Active Protection

Note

Active Protection is available for machines running Windows 7 and later, Windows Server 2008 R2 and later. Agent for Windows must be installed on the machine.

We recommend that you enable Active Protection on all machines that are not being throttled by lack of CPU resources.
Active Protection will typically have a few percents CPU overhead during heavy file access on the system.

Management Server self-protection

Make sure that the Management Server itself is also protected by a protection plan.

It is not strictly required to protect it because you can run a disaster recovery your entire environment using just our bootable media in isolation, but not having a backup of the Management Server will mean you have to reinstall the server, re-add each agent and redo the entire configuration after having restored your protected devices.

Having a backup of the Management Server will also enable such options as running it as a virtual machine or converting it into a virtual standby in order to accelerate recovery procedures (see Recovery recommendations section).

Storage considerations

As mentioned previously, a big consideration for large environments is the bandwidth of your centralized storage in regards to the number of concurrent backups saving data to this storage.

The resource usage calculator helps by providing an estimate on how many storage segments you will need to do a full backup of all your machines at the specified bandwidth and backup windows.

Deduplication

Deduplication is always at source in Acronis Cyber Protect, meaning that hash calculation is done by the agent and data already contained inside the backup is not resent over the network. This is a great way to reduce both storage needs and network bandwidth, especially if you are creating backups of similar machines.

Note that deduplication is a complex process that comes at the cost of using a moderately powerful storage server and lack of certain features, namely the lack of version 12 backup format support.

If you plan to use deduplication, definitely read more on deduplication technology and the best practices when using it in the Deduplication section of the User guide.

Deduplication makes the most sense when you are creating backups of many machines with a sizable percentage of identical data or when you need to store backups on a storage located on a WAN or other narrow bandwidth connection.

Deduplication and replication

The general recommendation is that replication should always be **to** a deduplicated location and never **from** a deduplicated one.

The reason behind this has to do with the fact that replication in Acronis Cyber Protect is not a simple copy of the archive data and acts more like a re-backup than a copy. This means that when you replicate to a deduplicated location, only the unique data is transferred, exactly as it would be for a backup. This is a major advantage if, for example, you are backing up locally and then replicating to an offsite deduplicated location.

This also means that data replicated from a deduplicated location is reconstituted during replication, meaning that the resulting file is no longer deduplicated and can be used in isolation from the deduplication service on the Storage Node.

This data reconstitution process causes a lot of overhead for the replication operation and it will take longer than if you were replicating from a non-deduplicated location. This will cause problems at scale, especially if the destination is a tape library and thus sensitive to delay.

Tape devices

Acronis is committed to continuing and expanded support for tape devices.

For a list of tested and supported tape devices, see the Tape hardware compatibility list.

To check the compatibility of your own tape devices, use the Tape compatibility tool.

If the tool finds a problem, please contact Acronis Support to get this escalated to the development and resolved.

An agent can create backups directly to tape. If you have a single or isolated machine and need to create tape backups, attach the drive directly to the machine that has the agent installed.

Storage Node for tapes

The Acronis Storage Node is required to create centralized backups from multiple agents to one or more tape drives. The tape device needs to be attached to the Storage Node.

If you plan to use both tapes and deduplication, the recommendation is to install a separate storage node for each storage as there is no practical limit to the number of storage nodes you can manage with one Management Server.

Tape management database

Information about all tape devices, tapes and the backup contents is stored in the tape management database located on the machine with the attached tape drive.

The default database path is:

- Windows 7, Server 2008 and later versions of Windows:
  %PROGRAMDATA%\Acronis\BackupAndRecovery\ARSM\Database
- Linux:
  /var/lib/Acronis/BackupAndRecovery/ARSM/Database

The database size depends on the number of backups stored on tapes and equals approximately 10 MB per hundred backups. This usually isn’t a problem for a few machines even for long retention periods.

However, please make sure you have enough space for this database on your system. If you are unsure, please change the path before starting any backups to tape.

To relocate the database in Windows

1. Stop the **Removable Storage Management** service.
2. Move all files from the default location to the new location.
3. Find the registry key **HKEY_LOCAL_MACHINE\SOFTWARE\Acronis\ARSM\Settings**.
4. Specify the new location path in the registry value `ArsmDmlDbProtocol`. The string may contain up to 32765 characters.
5. Start the **Removable Storage Management** service.

To relocate the database in Linux

1. Stop the **acronis_rsm** service.
2. Move all files from the default location to the new location.
3. Open the configuration file **/etc/Acronis/ARSM.config** in a text editor.
4. Locate the line `<value name="ArsmDmlDbProtocol" type="TString">`.
5. Change the path under this line.
6. Save the file.
7. Start the **acronis_rsm** service.

Warning!
Do not delete the tape database! This will result in rescanning all tapes to make the backups there usable again. This is a very long operation prone to errors.

Do not enable file recovery from disk backups

This option is disabled by default. Enabling it in your tape management protection plan options will add the ability to restore individual files from image backups stored on tape.

Note that this functionality comes at a steep storage space cost. If this functionality is enabled, at each backup the software creates supplementary files on a hard disk of the machine where the tape device is attached. File recovery from disk backups is possible as long as these supplementary files are intact. The files are deleted automatically when the tape storing the respective backups is erased, removed, or overwritten.

These supplementary files are located:

- In Windows 7 and later versions of Windows: **%PROGRAMDATA%\Acronis\BackupAndRecovery\TapeLocation**
- In Linux: **/var/lib/Acronis/BackupAndRecovery/TapeLocation**

The space occupied by these supplementary files depends on the number of files in the respective backup. For a full backup of a disk containing approximately 20,000 files (the typical workstation disk backup), the supplementary files occupy around 150 MB. A single full backup of a server containing 250,000 files may produce around 700 MB of supplementary files.

Even in small environments the size of such files will quickly grow to dozens of gigabytes.

The recommendation is to disable this option unless you absolutely need it and if this is the case, make sure that the Storage Node is sized keeping these supplementary files in mind.

Tape sets

Acronis Cyber Protect supports the creation of tape sets, which give you greater flexibility in managing which exact devices create backups to which tapes and the conditions under which this happens. For example, if you want to use a distinct tape every single day of the work week and then another set of tapes over the weekend.

Refer to the knowledge base article on tape sets at https://kb.acronis.com/content/59315.

Acronis Storage

Acronis Storage is a software-defined storage solution that allows you to quickly and easily transform low-cost commodity hardware and network equipment into the protected enterprise-grade storage like storage area networks (SAN) or network-attached storages (NAS).

Acronis Storage is optimized for storing large amounts of data and provides data redundancy (replication and erasure coding), high availability, self-healing, and storage sharing.

In Acronis Storage, user data is stored on organized clusters of servers in the form of fixed-size chunks. These chunks are automatically replicated and distributed across available servers in the cluster to ensure high availability of user data.

With Acronis Cyber Protect you can use an Acronis Storage cluster for your on-premises backups by registering an Acronis Storage Gateway in the product.

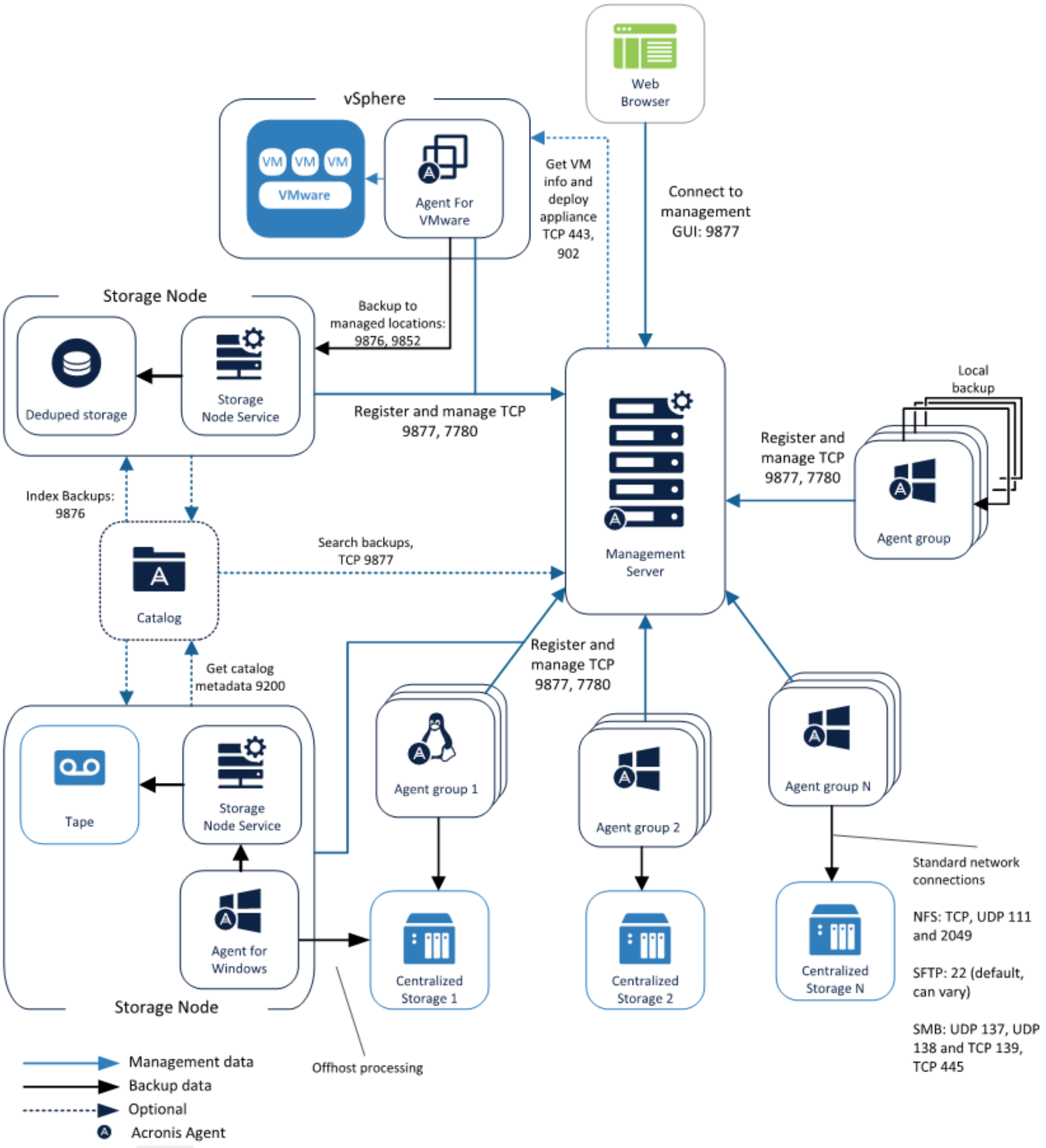
Note

This is the same exact storage solution as used in Acronis data centers for our cloud backups, and so has been proven to work well at scale. If your storage solution is not yet defined, Acronis Storage is a definite recommendation to store backups for large environments.

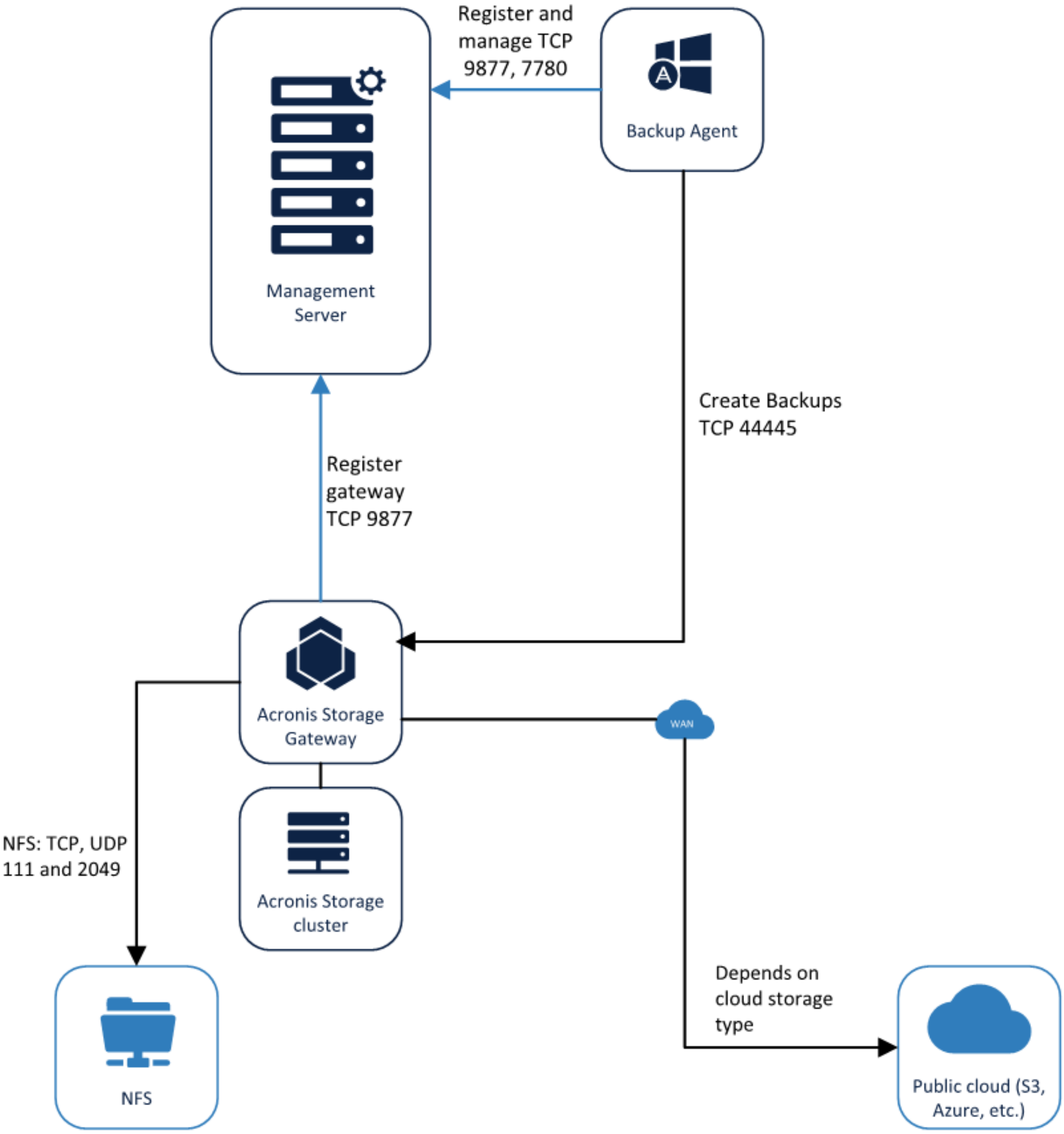
Network diagrams and ports

See the full network diagram in Appendix B.

Below is the network diagram for large environments.



Below is the network diagram for Acronis Storage.


Register and manage TCP 9877, 7780
Backup Agent
Management Server
Create Backups TCP 44445
Register gateway TCP 9877
Acronis Storage Gateway
WAN
Acronis Storage cluster
NFS: TCP, UDP 111 and 2049
NFS
Depends on cloud storage type
Public cloud (S3, Azure, etc.)

Recovery recommendations

This section contains some general recommendations and scenarios focused on recovering your environment.

If you are to follow a single recommendation in this document, the one you should always follow without question is to test and document your disaster recovery procedure. Testing on real hardware identical to production machines is preferred but not required. A test recovery procedure running on a virtual machine unrelated to your environment is still a lot better than not testing the procedure in the first place.

Bootable media

The Acronis Bootable environment is an immensely powerful tool; it lies at the core of the multitude of unique recovery scenarios offered by Acronis.

By default, this bootable environment takes the form of a lightweight Linux distribution created by Acronis. This distribution includes a fully-featured agent (same as any other installable agent), our own file system drivers and a GUI interface.

This environment can be used directly from the product. For example, if you restore a system image of a live machine from inside the Web console interface, the following process happens:

- The bootable environment image is written to a temporary location on the machine being restored.
- The recovery commands are written alongside the bootable environment. They will run after the bootable environment boots.
- The system on the machine is told to boot into the bootable environment on next reboot, and then we reboot the machine.

Another example is the **Acronis Startup Recovery Manager** (ASRM) which you can enable in order to boot into our Linux environment by pressing F11. You can find more details in the User Guide.

The most common scenario is to create a bootable media that runs this environment, either on legacy CD media or as an ISO, on a USB flash or PXE server. This media can be created by using the Acronis Bootable Media Builder or by downloading an ISO image directly from your account.

Testing the bootable media

It is absolutely vital to test the bootable media on your typical hardware before you actually use it to restore your system. So, if you have five different types of machines in your office, it is best to check on all five types. You need to check three things:

1. See if the media boots into your environment. If it doesn’t, recreate the media and try again. Most bootability errors are due to a faulty media or something having gone wrong during the creation process.

2. Check if all the local hard disks are properly detected. RAID devices should show up properly, for example, and not be seen on the level of the underlying disk structure.
3. Make sure that you can access your backup files from inside the media.

The reason for this is simple: the bootable environment on the media might not support your hardware. This doesn't happen often, but must be checked as one of the first things you do after setting up your backups.

Creating our own Linux distribution gives us unparalleled flexibility and provides unique features, but the downside is that we are always going to be limited in supporting hardware by open source driver availability in Linux. Since there is no general plug-n-play driver model for Linux, all the hardware drivers have to be compiled in advance when we create the bootable environment.

Some manufacturers simply do not provide a Linux driver for some of their hardware. In this case, there is nothing we can do to support it in the default Linux bootable environment.

More often, if something doesn't work, it is the case of using newer hardware, support for which has not yet been baked in to the bootable environment. Although we constantly update our Linux with the latest drivers, it is an impossible task for a third party to cover 100% of the new hardware being released each month.

If the media does not work correctly, please contact Acronis customer support to get this problem escalated to our Linux development team. Either a new version of the environment is already available that will support your hardware or we will create one, if this is possible. To contact the support, follow these instructions.

WinPE environment

Instead of using the default Linux environment, you can opt to use a Microsoft WinPE environment to create a bootable media. In this case the Acronis Bootable Media Builder will automate a standard process of creating a bootable WinPE image from the Windows ADK. The manual process described in the Microsoft knowledge base.

While creating the standard media, the Media Builder also install an Acronis Agent along with GUI so that it is available upon booting the media.

In most cases we recommend using the default Linux media since it is entirely under our control to fix something. For example, if our Linux environment has a problem booting, our engineers are able to debug and correct the issue. If the WinPE environment doesn't boot, there is nothing they can do because the media environment is entirely under Microsoft's control.

The main advantage of using WinPE is the fact that this Windows bootable environment supports all the same drivers available for the standard desktop system and you can add new drivers during media creation. Since hardware drivers are almost universally available for Microsoft Windows, the driver issue doesn't apply to the WinPE media as it does to our Linux environment.

With that in mind, we recommend using the WinPE media in the following cases:

- When you already use a WinPE based media for other things. If you already have a powerful bootable toolkit with all the plug-ins and tools your technicians know how to use, we recommend adding the Acronis agent on this same media to make it even more powerful.
- If you have hardware for which a Linux driver was never released by the vendor. For example, the Dell PERC S300 RAID controllers.
- If you have too many varied or constantly changing hardware configurations to protect. In this case, it can make more sense to create a media and add all the required drivers for all machines during media creation.

Automating media actions

A powerful feature of Acronis Cyber Protect is the ability to script bootable media backup and restore actions during creation. This allows you to automate the physical disaster recovery process and opens a number of interesting scenarios described later in this section.

If the environment you are protecting follows a typical hardware and protection plan template, we recommend making use of this functionality to formalize your disaster recovery procedure in the form of a scripted bootable media.

Not only will this be a good test of the recovery procedure, which you should always test beforehand, but will also allow efficient continued testing and reduction in RTO and personnel training. With a properly scripted media, the disaster recovery procedure on a single machine is simple enough for anyone to follow without having any prior knowledge of Acronis products.

For more information on adding automatic actions to the media, refer to the User Guide.

Registering the media

Another Acronis Cyber Protect feature which allows for unique backup and recovery scenarios is the ability to interact with the Agent on the Acronis media from the Web console as if it were a regular Agent for Windows or Linux (which it essentially is).

If you have need to run regular recovery scenarios, for example, you have a public workstation or school work PC that needs to be periodically restored from a golden image – we recommend you register the bootable media used on this machine in our Management server.

Once the media is registered, you will find it under the **Bootable media** tab under **Devices** and will be able to interact with it following the same workflow as for any other agent. For example, you can schedule backups to run on this media, you can configure and run a remote recovery, you can check the activities that ran on this media during the previous month, etc.

Each media is uniquely identified by a hash value created from the MAC addresses of the machine that boots this media. This means that a single CD or flash can be used to load any number of machines and each will be uniquely identified in the Management Server and this ID will remain consistent across any number of reboots as long as the NIC of this machine is not changed.

This recommendation also applies if you need to create backups without having to install anything on the operating system. For example, if you are using an unsupported legacy operating system like Windows NT (see Miscellaneous recommendations for details).

For instructions on registering the media, refer to the User Guide.

Recovery scenarios

Basic recovery

Basic recovery scenarios are described in detail in our documentation. They all have a common general recommendation: test your recovery procedure before you need it. You can find a summary list of all basic recovery scenarios in the User Guide.

Follow these instructions if you need to restore a single physical machine/virtual machine/file/application on an regular basis.

Mass recovery

This scenario describes the recommended configuration for situations where a mass, simultaneous recovery of all your machines is required. For example, if your company is under attack by a rapidly spreading virus, restoring machines one by one is not going to stave off the attack.

This scenario assumes that all your hardware is working and in place. For situations where you lose everything and need to run a disaster recovery in an offsite data center, see the Site-wide disaster recovery scenario.

Doing a mass recovery is not recommended over the network. Not only because it will be a bottleneck when recovering many machines at the same time, but also because we generally recommend shutting down the network as the first step when under attack by malware to prevent its further spread.

You can restore physical machines en masse without network access by following these recommendations:

- Set your protection plans to create a backup on the local storage of each machine.
  - For this scenario, you should set the retention rules to keep just the single latest backup locally, because you don’t need a full history on each machineю
  - The backups should be replicated to a centralized storage. Alternatively, you can create a second protection plan to run at a different time with different parameters. The local copies will be used to recover all the local machines as quickly as possible, the centralized copy will be used to recover a single machine that has stopped working.
- Optionally, create a scripted bootable media that will automate a recovery from this single local backup. This will save a lot of time and manpower.
- When disaster strikes, load each machine with the bootable media. Since the backup is local, you can load as many machines in parallel as possible. Each machine will start recovery on its own,

without affecting any other machines.
This is the quickest method for simultaneous disaster recovery of any number of physical machines.

Site-wide disaster recovery

This scenario provides recommendations for protecting against situations where you lose your entire environment and have to recover from offsite backups. This type of disaster happens far less often than a failing hard disk, but the consequences are far more destructive.

The biggest issue with recovering an entire environment is tied to the actual hardware running this environment. The backups are not sufficient in and of themselves unless you also have a place these backups can target for recovery.

Ideally, you should have a separate disaster recovery site sufficiently distant from your primary production location with enough hardware resources to run your production environment. This site should have regular annual disaster recovery drills.

Since this is an expensive endeavor, another good possibility is to have a virtual disaster recovery site, with enough VMware hypervisor resources to take the most critical production loads until the primary site is back online. Even if you have a physical disaster recovery site, it is highly recommended to have a good ESXi host or cluster to accelerate recovery.

Note
The current version of Acronis Cyber Protect offers more features for VMware compared to other virtualization platforms. If you have a choice of a Hypervisor for a disaster recovery site, go with VMware.

Finally, you can run an offsite disaster recovery on cloud servers, which has the major benefit of not requiring investment in stand-by hardware.

Acronis offers our own service that enables cloud disaster recovery:
https://www.acronis.com/business/disaster-recovery-service/

General recommendations for disaster recovery

Regardless of your DR site nature or locations, there are a number of general recommendations you should keep in mind when designing or running your disaster recovery scenarios.

The recommendations are grouped by offsite backup storage type because the steps necessary to run a recovery are different depending on where the backups are kept and certain types require preparation in advance.

Regular unmanaged or disk storage

In these locations, backup metadata in Acronis Cyber Protect is stored along with the actual backups. This makes the archives portable and the specific disaster recovery process simple.

From shipped USB disks on small environments, to SFTPs and large distributed SANs, you will be able to access these backups directly, from the Management Server, bootable media, or any other agent.

If your environment isn’t very large and the offsite backups are stored on disks shipped to a physical DR location, the recommended recovery procedure is much the same as the one described in the Mass recovery section. Simply plug in the disk containing your backups to the machine, load the media and restore from the attached disk to the internal one.

For larger physical environments with unmanaged storage locations, the recommendation is to follow this template:

- Restore your backup of the Management Server.
- Add the backup location to your Management Server.
- Boot each machine that requires recovery from the media and register it on the Management Server.
- Start the different recovery procedures remotely from the Management Server once these machines start appearing in the interface.
- If you have more than a pair of hands running the recovery, do not wait for the Management Server to go online and start registering bootable media agents. Start parallel recovery operations from multiple copies of the bootable media.

Note that the machine will not necessarily appear as an online device in the Management Server UI after recovery. The recovered agent will keep trying to reach the old address and host name. You can either re-register the agent after recovery to continue protection management on the disaster recovery environment, or make sure that the recovered Management Server has the same name and address as the old one.

If you have a vSphere/ESXi on your disaster recovery site, the basic workflow is a bit different:

- First, we recommend storing a virtual machine copy of your management server in advance. You can create a copy by running a regular **Convert to VM** offsite job which targets your Hypervisor.
- When running the DR procedure, the first step would be to simply power on this Management Server virtual machine.
- Once the virtual machine is up and running, add or refresh the offsite backup storage.
- Register the vSphere/ESXi to the Management Server running on this environment.
- For the priority infrastructure, choose the **Run as VM** option to get it back up and running in minutes as virtual machines. Running the machine as a virtual machine doesn’t copy the data back to the datastore, the system just mounts it and uses directly. This running virtual machine can be moved to production without requiring downtime, a unique feature to Acronis Cyber Protect.
- The other, less critical machines, can be recovered using the methods described above.

Managed locations (including deduplication)

The big difference with managed locations is the fact that the backup metadata is kept on the Acronis Storage Node. This is critical especially when using deduplication, because this metadata is required for restoration and takes a long time to recreate.

This means that for any offsite managed storage location, it is recommended to keep the Storage Node strictly on the same offsite location as the storage medium itself and then register this Storage Node across the WAN.

When using this recommended configuration, the regular procedures remain valid with a simple modification:

- After restoring the Management Server, re-register this Storage Node on the restored server. The backups will become accessible exactly as they were for the onsite Management Server since the Storage Node is self-contained.

Note that you can also access any Storage Node location directly from the media without having to go through the Management Server. Just type `bsp://storage.node.address/` in the location path in the restoration window (`bsp` stands for “backup storage protocol” and it is the Acronis protocol used by the Storage Node to communicate with agents).

Tapes shipped offsite

Tape metadata is also stored on the Storage Node. This tape index data is required to restore the backup. The fact that it can take days to rescan a large number of tapes before you can recreate the metadata and make proper use of them means that being prepared in advance is especially critical for this type of environment if you are protecting more than a few servers.

The critical step in preparing for this scenario is simple: make sure that the backup of Storage Node tape database is kept in the same location as your offsite tape storage. And each time you ship tapes offsite, make sure to ship an updated backup copy of the Storage Node. The backup can be kept on tape or on any other media. For example, keeping a copy in the cloud is a good alternative if your secondary location is accessible via WAN. Since you only need a copy of the system and its metadata, the Storage Node backup shouldn’t take up much space.

If you are storing the Storage Node backup on tape along with the other shipped tapes, please make sure to mark this tape in an appropriate manner.

- The first step in your recovery procedure will be to restore this backup of the Storage Node to a new machine from the bootable media. This involves rescanning the tape from inside the media, after which the recovery points will be available in the bootable environment interface.
- Once the Storage Node is restored along with the tape database, you can make use of subsequent tapes without having to rescan them, saving you many hours of time.
- Once the tape Storage Node is back to a usable state, you can use the same exact procedure as described in the previous section for managed locations.

Miscellaneous recommendations

This section includes a number of miscellaneous recommendations that aren't tied to specific environment details.

Backing up an unsupported operating system

This section also applies to supported systems where you aren't able to install an agent due to security policy or other reasons.

Acronis Cyber Protect image backups work on a low disk block level, meaning that an "unsupported" operating system with a supported file system can still be backed up as long as you can cover this file system by an agent capable of running this backup.

By unsupported systems, we refer to all operating systems inside which an agent cannot be installed. This usually happens because the new version of the agent has library dependencies that cannot be met by legacy systems. We try very hard to support older systems – we are one of the few solutions that allow you to install an agent on Windows XP, for example, but there will always be a limit to how far back you can go.

However, as mentioned in the previous section, our bootable environment contains a standalone agent. This agent is entirely independent of the operating system installed on the disk that is being backed up. As long as the agent is able to back up the file system, you can use it without installing anything.

Even if the file system is unsupported, you can still back it up by using the **sector-by-sector** option. The only requirement is that this be an undistributed file system based on block devices. This method will copy each block from the original disk, including the free space.

The procedure to protect these systems is as follows:

1. Boot the system using our media and register it on the Management Server as described in the recovery recommendations section.
2. Create a protection plan on this bootable media.
3. Reboot the machine and run the plan anytime you need to run a backup.
   Rebooting the machine on schedule is not yet possible directly from the product, so this process cannot yet be entirely automated from inside Acronis Cyber Protect.

Backing up mobile endpoints

There are a number of specifics related to creating backups of laptops and notebooks. For example, you don't want the backup to run when the device is connected via a VPN or on a metered connection.

In order to better serve these scenarios, there are a number of specific scheduling options and start conditions.

Scheduling options:

- Waking up a machine for backup from the sleep or hibernation mode
- Prevention of the sleep or hibernation mode during a backup
- The option to prohibit running missed backups on a machine startup

Backup start conditions:

- Do not start when on battery
- Start when on battery if the battery level is higher than
- Do not start when on metered connection
- Do not start when connected to the following Wi-Fi networks
- Check device IP address

Make sure to use these conditions when creating centralized backup policies of your laptops and tablets.

For detailed description of these options, refer to the User Guide.

Backup location defined by script

This is a powerful feature for creating a parametrized backup location. For example, if you have a number of machines and each one has to be backed up in its own specific folder (like the machine name).

Instead of creating a backup for each machine, the recommendation in this case is to use a script that will resolve the location in a single plan. Scripts can be written in JScript or VBScript. When deploying the protection plan, the software runs the script on each machine. The script output for each machine should be a string containing a local or network path. If a folder does not exist, it will be created. On the **Backup storage** tab, each folder will be shown as a separate backup location. For network folders, specify the access credentials with the read/write permissions.

For example, the following JScript script outputs the backup location for a machine in the format `\\bkpsrv\<machine name>`:

```
WScript.echo("\\\\bkpsrv\\" + WScript.CreateObject("WScript.Network").ComputerName);
```

As a result, the backups of each machine will be saved in a folder of the same name on the server `bkpsrv`.

Compression and encryption

Compression

Acronis Cyber Protect uses a compression algorithm called Zstandard (or Zstd).

Even on normal compression settings, this algorithm provides better compression ratios than the previously used Zlib on high settings, all while being faster.

We recommend that you keep the default compression settings as the best balance between space savings and backup performance.

Encryption

Encryption settings are specified when creating a protection plan and cannot be modified later. You will have to recreate a new protection plan to use different encryption settings.

There are three levels of encryption available:

- AES 128
- AES 192
- AES 256

The level of encryption is a trade-off between security and backup performance on the agent. Encryption usage, especially at higher levels, takes time and CPU resources.

Since encryption can have an impact on your backup times even at lower settings, we recommend using it judiciously:

- Always encrypt backups sent offsite or to the cloud
- Encrypt backups that contain sensitive data, such as medical records or customer data

Note
Note that the password needs to be provided for every recovery operation and cannot be recovered if lost.

You can also use encryption as a machine property. For more details, check out our documentation on the link below:

https://www.acronis.com/support/documentation/AcronisCyberProtect_15/#37608.html

Security hardening

Security hardening recommendations are available in a separate document, the Security Hardening Guide.

Appendix A. Services

Services and components

Visit our Knowledge Base for a list of ports, services, and processes that Acronis Cyber Protect uses:

- For Windows, see Acronis Cyber Protect 15: Windows services and processes (https://kb.acronis.com/content/65663).
- For Linux, see Acronis Cyber Protect 15: Linux components, services, and processes (https://kb.acronis.com/content/67276).

Service Accounts

The majority of the services listed above are installed and run under Network Service or Local System service users.

However, you can specify your own service users for three services in the product:

1. Acronis Managed Machine Service on the agent.
2. Acronis Management Server Service on the Management Server.
3. Acronis Storage Node Service on the Storage Node.

By default, the Managed Machine Service on the agent is installed and runs under the **Local System** account. The Management Server and Storage Node services are installed with new users created by our installer called **AMS User** and **ASN User** respectively.

However, you can change the service user as an installation option by selecting **Use the following account**. This option is forced if you are installing on a domain controller, because the installer cannot create new accounts on a domain controller for security reasons.

New accounts are created with random GUID passwords.

These users are assigned the following rights and privileges during installation:

Acronis Managed Machine Service

- Included in the Backup Operators and Administrators groups.
  Administrator group membership is granted only if this is a new user. Existing users are not granted this membership.
- Granted the **Full Control** permission on the folder %PROGRAMDATA%\Acronis (in Windows XP and Server 2003, %ALLUSERSPROFILE%\Application Data\Acronis) and on its subfolders.
- Granted the **Full Control** permission on certain registry keys in the following key: HKEY_LOCAL_MACHINE\SOFTWARE\Acronis.
- Assigned these user rights:
  - Log on as a service.
  - Adjust memory quotas for a process.

- Replace a process level token.
- Modify firmware environment values.

Acronis Management Server Service

- Included in the Acronis ApiGatewayUsers and Acronis Centralized Admins groups.
  These groups are created during installation and are used for group and user management inside the product.
- Granted the **Full Control** permission on the folder %PROGRAMDATA%\Acronis (in Windows XP and Server 2003, %ALLUSERSPROFILE%\Application Data\Acronis) and on its subfolders.
- Granted the **Full Control** permission on certain registry keys in the following key: HKEY_LOCAL_MACHINE\SOFTWARE\Acronis.
- Assigned these user rights:
  - Log on as a service.

Acronis Storage Node Service

- Included in the Backup Operators, Administrators, Acronis Centralized Admins groups.
  Administrator group membership is granted only if this is a new user. Existing users are not granted this membership.
  Acronis Centralized Admins group is created during the installation.
- Granted the Full Control permission on the folder %PROGRAMDATA%\Acronis (in Windows XP and Server 2003, %ALLUSERSPROFILE%\Application Data\Acronis) and on its subfolders.
- Granted the Full Control permission on certain registry keys in the following key: HKEY_LOCAL_MACHINE\SOFTWARE\Acronis.
- Assigned these user rights:
  - Log on as a service.

Credential storage

Credentials are stored on the filesystem in the **C:\ProgramData** folder. They are encrypted using AES-256-CBC. The encryption key is created per following service:

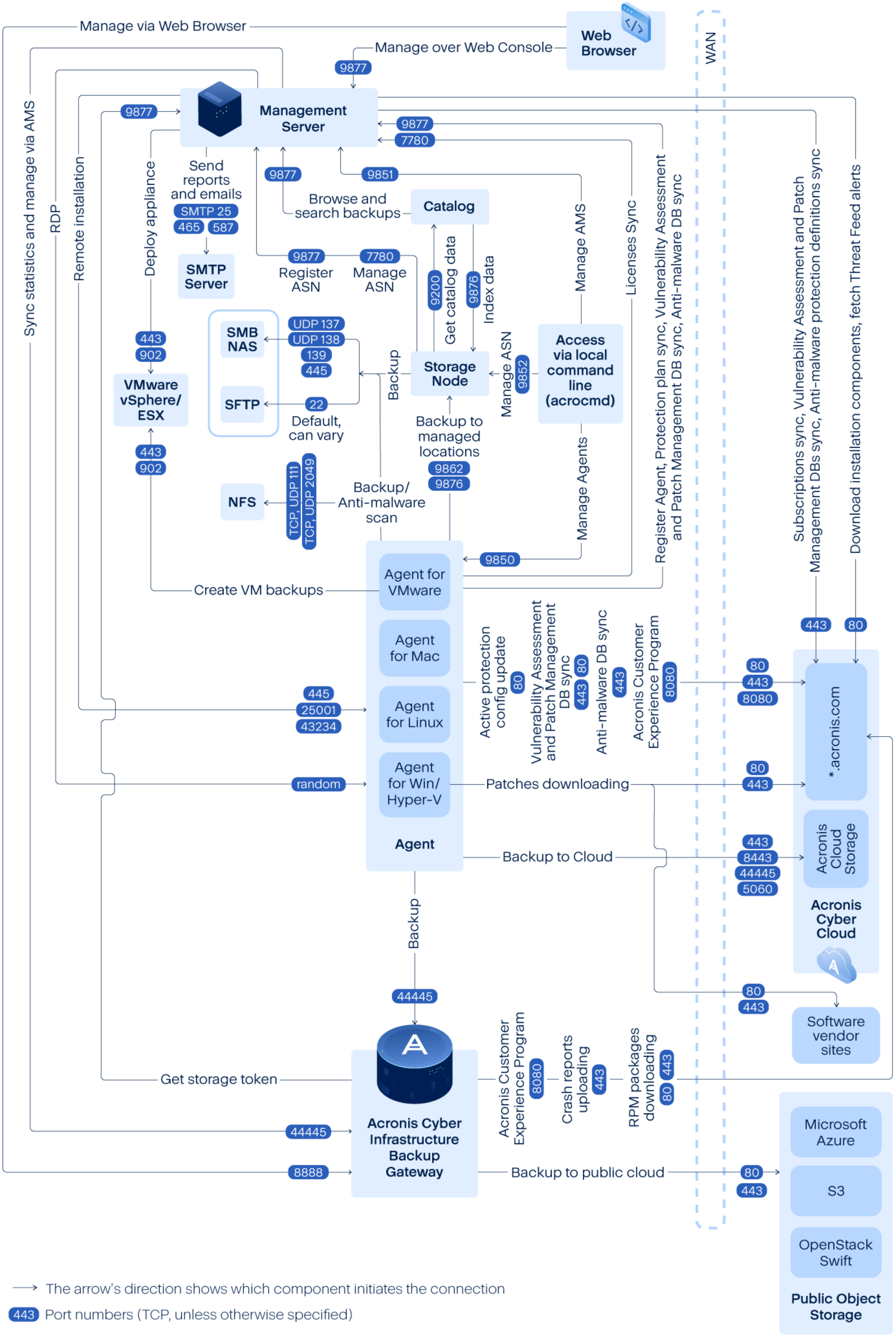
- Acronis Management Server service
- Managed Machine service
- Acronis Storage Node service

If all three services are installed on the same server each will use its own different credential storage and encryption key.

This key is generated as follows:

- A random high-entropy "machine key" is generated during an installation procedure.
- This machine key is used to derive the actual encryption key using an algorithm implemented inside the credential storage application.

Appendix B. Network diagram and ports



⟶ The arrow's direction shows which component initiates the connection

443 Port numbers (TCP, unless otherwise specified)

The vulnerability assessment for Linux is implemented via a CVSS service deployed in Acronis Cyber Cloud. Protection agents choose dynamically the closest Data Center via ping from the list https://cloud.acronis.com/services.json.

Appendix C. Performance Reference

Backup performance reference

This topic contains information about normal system performance during back up. The performance results cover the most frequent use cases and do not include all possible combinations of backup settings. The results are applicable to the supported configurations that are described in the Hardware requirements and sizing sections of this guide.

Note

The values in this article are aggregate mean ranges for all supported environments - individual, small, SMB, and large. The actual performance in your environment might vary depending on your network bandwidth and traffic, the number of concurrent backup jobs, the speed of your storage devices, the size of your files related to the stripe size, and so on.

For optimal results, always use the normal compression level. If you are concerned about the size of the resulting archive, use the high compression level.

Storage and Network Parameters

The following table contains information about the storage and network used in the performance testing.

Parameter	Source server	Destination server
Hard Drive type	SSD	SSD
RAID configuration	RAID0	RAID0
Stripe size	1 MB	1 MB
Caching	On	On
Disk cache policy	Always read ahead	Always read ahead
Write mode policy	Write back	Write back
Cache for physical device	Off	Off
SAN architecture	10 Gbit Fibre Channel	10 Gbit Fibre Channel

File backup performance results

The backup options that are not mentioned in the table are set with default values.

Backup type	Individual file size	Number of files	No compression	Normal compression	High/Maximum compression

		in the backup source (Total Archive size)						
			Speed (Mbps)	Total time (sec)	Speed (Mbps)	Total time (sec)	Speed (Mbps)	Total time (sec)
Full file backup	1 GB	200 (200 GB)	428	201	425	505	202	1062
Incremental file backup Changes were done in 50% of each file	1 GB	200 (200 GB)	426	252	418	257	207	518
Full file backup	712 KB	294543 (209 GB)	318	676	315	681	106	2031
Incremental file backup Changes were done in 50% of each file	712 KB	294543 (209 GB)	403	266	404	266	227	472

Disk backup performance results

The backup options that are not mentioned in the table are set with default values.

Backup type	Individual file size	Number of files in the backup source	No compression		Normal compression		High/Maximum compression	
			Speed (Mbps)	Total time (sec)	Speed (Mbps)	Total time (sec)	Speed (Mbps)	Total time (sec)
Full disk backup	1 GB	200 (200 GB)	523	411	523	411	302	712
Incremental disk	1 GB	200 (200 GB)	487	221	486	221	289	371

backup Changes were done in 50% of each file								
Full disk backup	712 KB	294543 (209 GB)	520	414	520	414	301	715
Incremental disk backup Changes were done in 50% of each file	712 KB	294543 (209 GB)	219	490	219	491	218	492

Recovery performance reference

This topic contains information about normal system performance during recovery. The performance results cover the most frequent use cases and do not include all possible combinations of recovery settings. The results are applicable to the supported configurations that are described in the Hardware requirements and sizing sections of this guide.

Note

The values in this article are aggregate mean ranges for all supported environments - individual, small, SMB, and large. The actual performance in your environment might vary depending on your network bandwidth and traffic, the number of concurrent recovery jobs, the speed of your storage devices, and so on.

Storage and Network Parameters

The following table contains information about the storage and network used in the performance testing.

Parameter	Destination server	Source server
Hard Drive type	SSD	SSD
RAID configuration	RAID0	RAID0
Stripe size	1 MB	1 MB
Caching	On	On

Disk cache policy	Always read ahead	Always read ahead
Write mode policy	Always write back	Always write back
Cache for physical device	Off	Off
SAN architecture	10 Gbit Fibre Channel	10 Gbit Fibre Channel

File recovery performance results

The recovery options that are not mentioned in the table are set with default values.

Recovery type	Individual file size	Number of files in the source to recover	Source archive file with no compression		Source archive file with normal compression		Source archive file with high compression	
			Speed (MBps)	Total time (sec)	Speed (MBps)	Total time (sec)	Speed (MBps)	Total time (sec)
File recovery with file backup without overwrite (The target disk was formatted before the recovery operation)	1 GB	200 (200 GB)	249	864	248	865	254	845
File recovery with file backup without overwrite (The target disk was formatted before the recovery operation)	712 KB	294543 (209 GB)	166	1295	165	1301	167	1287
File recovery	1 GB	200	-	-	253	850	247	869

from incremental backup archive (The target disk was formatted before the recovery operation)								
File recovery from incremental backup archive (The target disk was formatted before the recovery operation)	712 KB	294543	-	-	161	1337	159	1350

Volume recovery performance results

The recovery options that are not mentioned in the table are set with default values.

Recovery type	**Individual file size**	**Number of files in the source to recover**	**Source archive file with no compression**		**Source archive file with normal compression**		**Source archive file with high compression**	
			Speed (MBps)	**Total time (sec)**	**Speed (MBps)**	**Total time (sec)**	**Speed (MBps)**	**Total time (sec)**
Full Disk recovery The target disk was formatted before the recovery operation	1 GB	200 (200 GB)	542	403	541	404	543	403
Full Disk	712 KB	294543	539	407	537	408	540	406

recovery The target disk was formatted before the restore operation		(209 GB)						
Full Disk recovery from incremental backup archive The target disk was formatted before the restore operation	712 KB	294543	418	521	418	521	418	521

Index