Acronis

Security Hardening Guide

Revision: 09/10/2020

Table of contents

1 Installation

It is highly recommended to use the recent Acronis Cyber Protect 15 update, as it may include the important security fixes and improvements.

If you install Acronis Management Server in the Windows environment, it is recommended to install it on any virtual machine or hardware node except the Domain Controller.

It is not recommended to change the accounts under which the services run (https://www.acronis.com/support/documentation/AcronisCyberProtect_15/index.html#40078.html).

If you have Active Directory, use managed service accounts (https://docs.microsoft.com/en-us/windows-server/security/group-managed-service-accounts/group-managed-service-accounts-overview) so that you do not have to change the credentials on all machines.

Installation recommendations

There are three types of Acronis Cyber Protect installation:

- Web installation. It is a small setup file that downloads the remaining components after it is launched. You need Internet access every time you want to install the software by using the web installer. The drawback is that the web installer can cause problems with system infection by viruses or threats.
- Remote installation.
- Offline installation.

The recommended method is offline installation. The installation package can be placed on a network share or Microsoft System Center.

If you do not deploy the Acronis Storage Node, then the Catalog is not required to be installed.

Agent registration recommendations

For security reasons, it is recommended to disable the anonymous registration on the Management Server. To learn how to do this, refer to Configuring anonymous registration (https://www.acronis.com/support/documentation/AcronisCyberProtect_15/index.html#42457.html).

The agent can be registered in two ways:

1. By using the registration token.

   You need to generate a registration token in the backup console. Then, on the machine to be protected, run the following command to register the backup agent in the Acronis Management Server:

```
<path_to_the_cyber_protection_agent_installer>\AcronisCyberProtect_15_64-bit.exe
--add-components=agentForWindows --reg-address=<management_server_address>
--reg-token=<token_generated_in_the_backup_console>
```

   You can use the registration token in the MST files for an automated backup agent deployment.

2. By using the user name and password.

The recommended method is using the registration token.

2 Operations

2.1 Backup security

It is recommended to encrypt your backups. As a result, a backup will be stored encrypted at rest and a user will have to enter the encryption password in order to restore or view the saved encrypted backup.

For more details how to encrypt backups, refer to the Acronis Cyber Protect 15 web help (https://www.acronis.com/support/documentation/AcronisCyberProtect_15/#37608.html).

2.2 Recommended backup destinations

You can choose the backup destination that will be appropriate to your security risk model, as outlined in the following table:

Destination	Security protocols	Tenant isolation capability
Cloud storage	TLS, client-server certificate	yes
Local folder	–	no
Network folder	SMB/CIFS	no
Acronis Cyber Infrastructure	TLS, client-server certificate	yes
NFS folder	–	no
Secure zone	–	no
SFTP	SSH2	no
Acronis Storage Node	TLS	no

2.3 Administrator assignment

For security reasons, it is highly recommended to limit the list of administrators who can fully manage Acronis Cyber Protect.

The recommended way of assigning an administrator is a group in Active Directory.

2.4 Organization units

Organizing the structure

With the Advanced license, it is possible to create organizational units and add administrators to them. This allows you to delegate backup management to other people whose access permissions will be strictly limited to the units assigned to them.

Administrator accounts can be created at the unit or organization level. Each account has a view scoped to their area of control. Users only have access to their own backups.

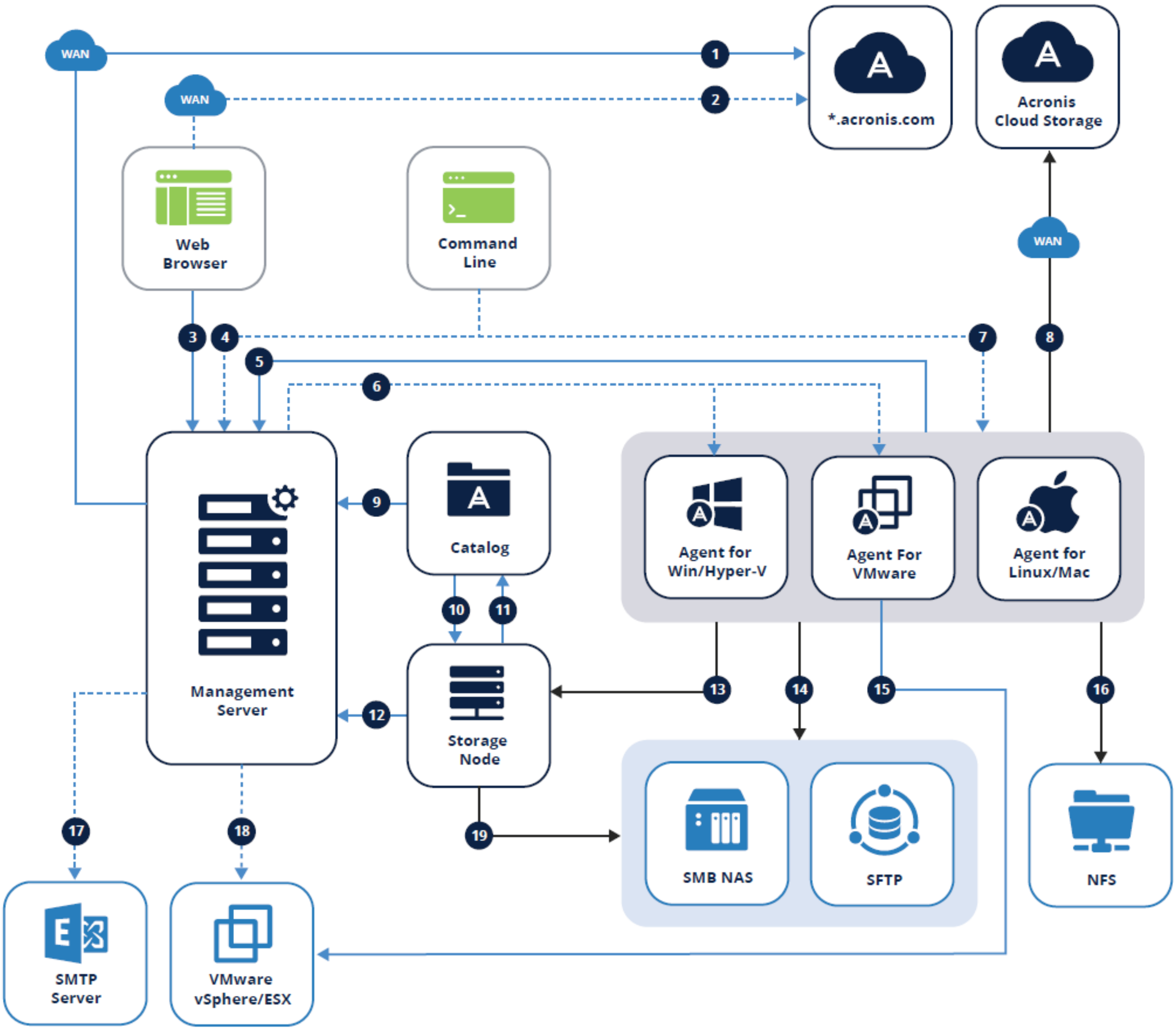
To learn more about the types of administrators and their control area, refer to the Acronis Cyber Protect 15 web help.
(https://www.acronis.com/support/documentation/AcronisCyberProtect_15/index.html#39120.html
)

3 Secure network configuration

This section describes the network configuration for secure communications between Acronis Cyber Protect components.

3.1 Network security diagram

On the diagram below, you can see the network security diagram which shows Acronis Cyber Protect 15 components and communications between them. For security reasons all the ports are closed except those that are listed in the table below.



The arrow direction shows which component initiates the connection. Note that all ports are TCP unless otherwise specified.

1. Download installation components: 443 to dl.acronis.com 🔒	**12.** - Manage ASN: 7780 ZMQ 🔒 - Register ASN and manage tasks: TCP 9877
2. Sync subscription licenses: 443 to account.acronis.com 🔒	**13.** Backup to managed location: 9876,9852 🔒

3. Manage Environment: 9877 🔒	**14.** - SMB: UDP 137, UDP 138 and TCP 139, TCP 445 - SFTP: 22 (default, can vary)
4. Access via remote CL (acrocmd, acropsh): 9851	**15.** Create VM backups: 443, 902
5. - Register Agent: 9877 - Manage Agent: 7780 ZMQ 🔒 - Sync licenses: 9877	**16.** NFS: TCP, UDP 111 and 2049
6. Remote installation: **U1 and earlier**: 445, 25001, 9876 **U2+**: 445, 25001, 43234	**17.** Send reports and emails: SMTP (25, 465, 587, etc)
7. Access via remote CL (acrocmd, acropsh): 9850	**18.** Deploy Appliance: 443, 902
8. Create backups to Acronis cloud storage: 443, 8443, 44445, 5060	**19.** - SMB: UDP 137, UDP 138 and TCP 139, TCP 445 - SFTP: 22 (default, can vary)
9. Browse and search backups: 9877	
10. Index backups: 9876	
11. Receive catalog metadata: 9200	

→	Backup data	🔒	CurveZMQ 256-bit key
→	Management data	🔒	HTTPS/TLS
⇢	Optional functionality		

3.2 Ports

This section lists the different ports that should be opened for communication between the different Acronis components inside the network as well as traffic to the outside. These are same ports as used in the diagram above, but presented in a list by component.

Note that all communication between the many services of a single component are also done through network connections. These services listen exclusively on localhost and the ports are not listed here because nothing needs to be opened in the firewall or otherwise changed in your network.

Though these internal ports do not affect traffic, they can create a conflict if another application is listening on the same port. You can usually change the internal port used by Acronis services in the .json configuration file for the service found in its directory in ***c:\Program Files\Acronis\[service_name]\[service_name].json***

Management Server

The following ports should always be opened on the Management Server for incoming connections from different components:

- TCP 9877 (API gateway)
- TCP 7780 (for communication with the agents)
- 9850 (ASYNC IPC)

The following ports are optional if you want to access the Management Server from the remote command line:

- TCP 9851

Protection Agents

Agents do not require any open ports for regular backup and restore functionality. Optionally, open the following ports for remote installation and remote access via the command line:

- TCP 445, 25001, 9876 (Remote installation, for communication with the Storage Node)
  TCP 445, 25001, 43234 (Remote installation)
- TCP 9850 (Access via the remote command line acrocmd)
- TCP 44445, 443 (for backup to the cloud)
- TCP 9877 (for mini-plans)

Storage Node

The Storage Node requires the following incoming ports to be open for communication with agents:

- TCP 9876, 9852

The following ports need to be opened for communication with the Catalog, if it is installed separately:

- TCP 9876

Catalog

If the Catalog is installed separately, it needs to be able to accept incoming connections from all Storage Nodes on the following port:

- TCP 9200

Outgoing WAN connections

If you are using Acronis cloud functionality, the firewall has to allow outgoing connections to the following ports:

- TCP 80 (download installation files from UI)
- TCP 443 (sync licenses with account.acronis.com – this is required for subscription licenses)
- TCP 443, 8443, 44445, 5060 (create backups to Acronis cloud storage)

Third party components

Acronis products need to communicate with outside components for certain functionality. For example, your SMTP server must accept connections from the Management Server in order to make use of the email notification functionality. This section lists the most commonly used components and their ports:

- **VMware**: TCP 443, 902 (need to be open for all connections from Acronis components that communicate with vSphere/ESX)
- **SMTP**: Default ports include TCP 25, 465, 587, etc (from AMS to mail server, value can vary)
- **NFS**: TCP, UDP 111 and 2049 (from agents to NFS host)
- **SMB**: UDP 137, UDP 138 and TCP 139, TCP 445 (from agents to SMB share)
- **SFTP**: default TCP 22 (can vary depending on your server configuration)