ABR11.5 Network Connections

1. Remote installation of Agents

Management Server is present

Management console — TCP 9876: Requesting to install components → Management server

TCP 9876: Registration on the management server

TCP 445: Sending files (see the list)

TCP 25001: Sending installation parameters

TCP 22 (SSH): Sending files (see the list) Starting installation

License server — TCP 9876: Acquiring a license
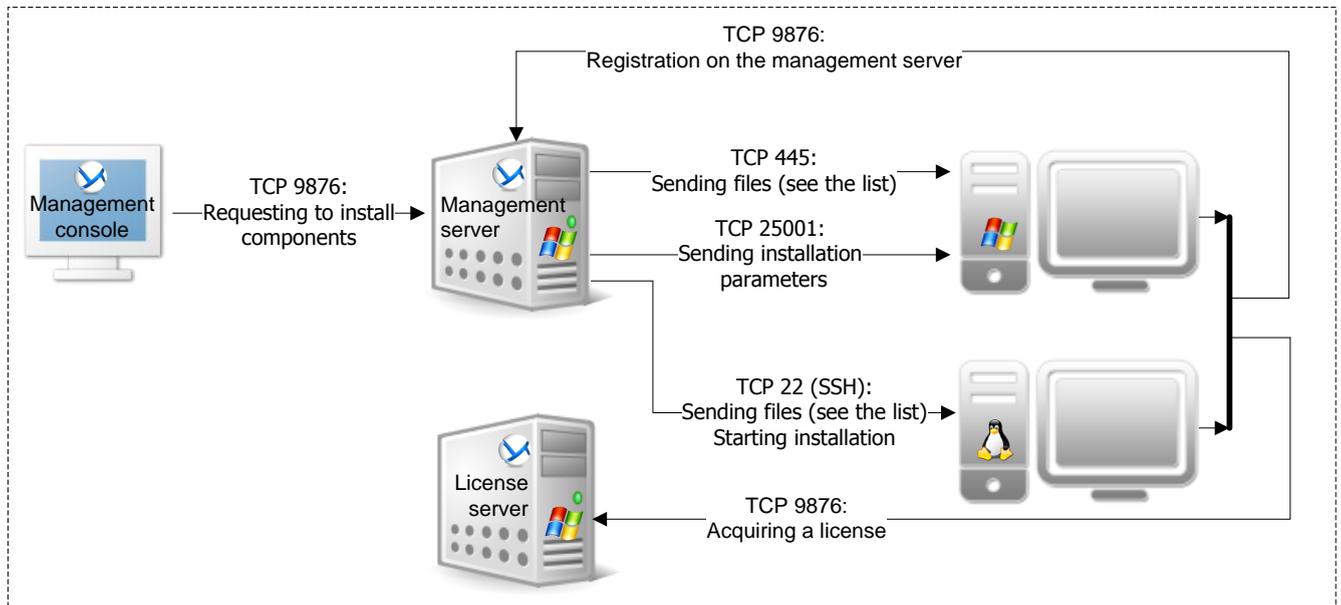
Management Server is absent

Management console

TCP 445: Sending files (see the list)

TCP 25001: Sending installation parameters

TCP 22 (SSH): Sending files (see the list) Starting installation

License server — TCP 9876: Acquiring a license (Use of the license server is optional.)
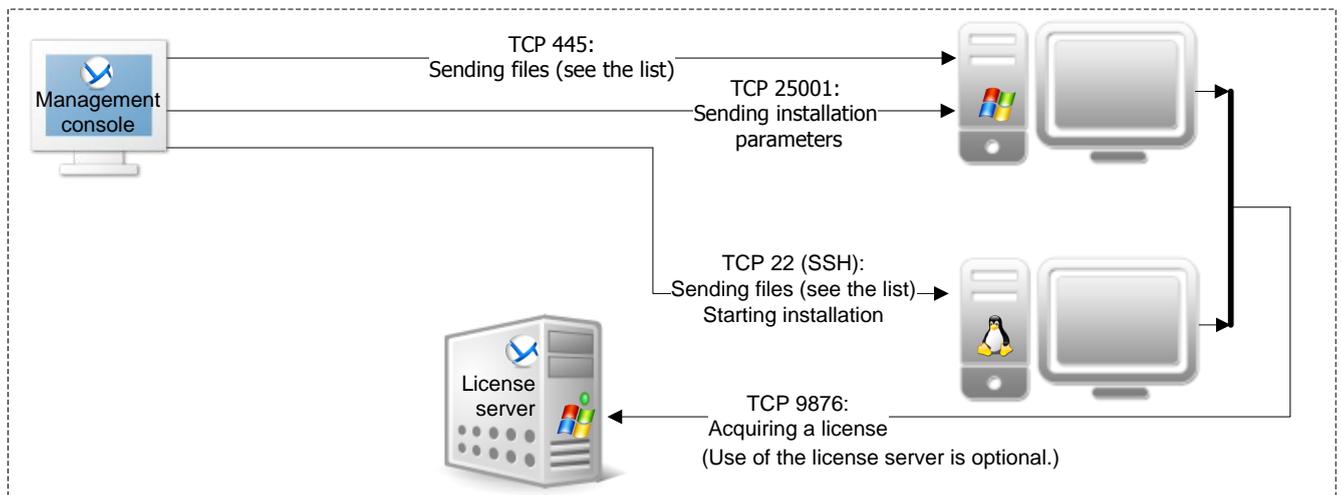
Connection notes:

- ➜ **:** The arrow direction shows which component initiates a connection. The text shows the destination port. The source port is 1025–5000 (Windows prior to Windows Vista), 49152–65535 (Windows Vista and later), or 32768–61000 (Linux and the virtual appliance).

- The agent registers itself by using the specified network name or IP address of the management server. If the network name is specified, the agent obtains the IP address either from the DNS server or from the hosts file (**%SystemRoot%\system32\drivers\etc\hosts** in Windows or **/etc/hosts** in Linux). Adding the management server to this file helps when the agent is located on a different subnet than the management server.

- In a non-DNS environment, it is necessary to enable **Network Discovery** and **File and Printer Sharing** on the machine from where the installation is performed (the management server or the management console). This requires additional TCP and UDP ports to be open.

Encryption notes:

- **TCP 22**: Traffic is encrypted by using the SSH protocol.
- **TCP 445:** Traffic encryption depends on the File and Printer Sharing options in Windows
- **TCP 9876:** By default, traffic is encrypted. Encryption is configured through the Acronis administrative template.
- **TCP 25001:** Traffic itself isn't encrypted. But all user names and passwords are sent encrypted.

List of transferred files (Windows):

- **Installation packages (.msi files)**: Contain components being installed
- **Acroinst.exe:** Manages the installation process
- **Msi_setup.exe:** Installs a component

List of transferred files (Linux):

- **Installation packages (.i686 or .x86_64 files)**

2. Communication between components

Encryption notes:

- 🔓**:** Traffic is not encrypted.
- **TCP 9876:** By default, traffic is encrypted. Encryption is configured through the Acronis administrative template.
- **TCP 443:** Traffic is encrypted by the HTTPS protocol.

Connection note:

- ➤**:** The arrow direction shows which component initiates a connection.

* **Registering:** Connection is initiated by either the management server or the agent, depending on which component triggers the registration process.
Managing: *The management server* initiates a connection to deploy centralized backup plans and collect logs. *An agent* initiates a connection to notify that the machine has come online or that its IP address has changed.