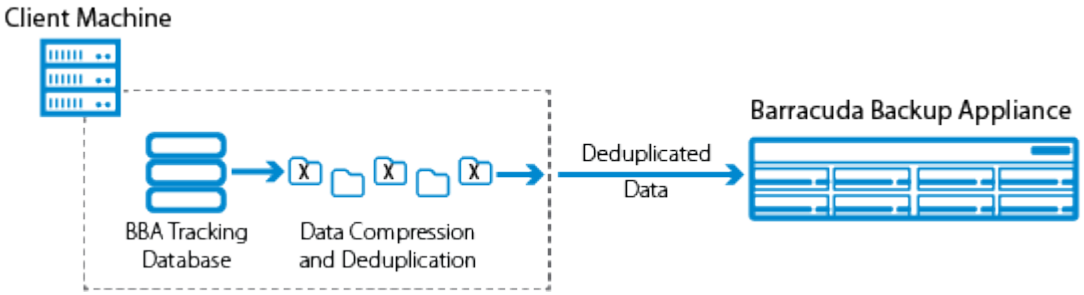
Barracuda Backup Agent for Windows, macOS, and Linux

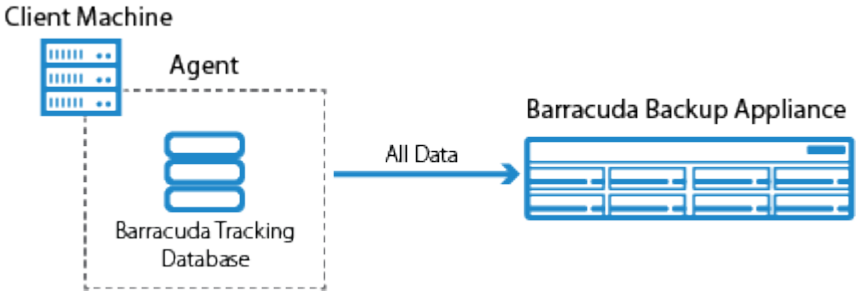
https://campus.barracuda.com/doc/78809295/

The Barracuda Backup Agent provides source-based deduplication by breaking down large files into smaller chunks before sending them to the Barracuda Backup device. During agent installation, a small database is created on the server to keep track of data chunks so only unique data is compressed, encrypted, and sent to the local Barracuda Backup device for processing, reducing network traffic and the backup window. Prior to the files being sent to the Barracuda Backup device, each file part or chunk is hashed using a combination of MD5 and SHA1 algorithms. This process identifies all blocks of data, verifies data integrity, and detects errors. Redundant data blocks are replaced with a pointer to the unique data block stored on the Barracuda Backup device. The end result is that only the required unique data blocks are ever written to disk and only written a single time:



The Barracuda Backup Agent provides protection for open files and file permissions (ACLs). Once installed, the Barracuda Backup Agent runs in the background on your server, listening for TCP connections on port 5120. When a backup is run on a data source protected by the Agent, the Agent performs the following operations:

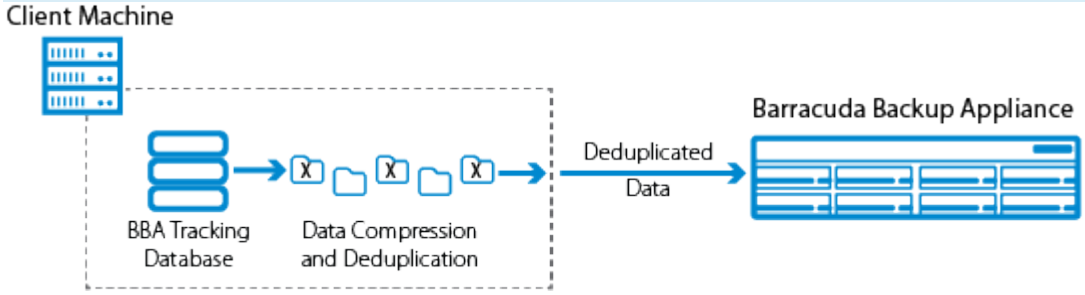
- **First-Pass Backup** – The first backup performed on a machine running the Agent. At the beginning of a first-pass backup, the Barracuda Backup database has no data for the system being backed up and therefore the Barracuda Backup Agent databases are also empty, meaning every file must be sent to the Barracuda Backup device. Deduplication still occurs during the job against data parts sent earlier in the job or against parts from other systems being backed up.



- **Second-Pass Backup** – A backup job (or a subset of selections within a job) for which the

Agent must rescan the source filesystem and check its database to see if a file has been modified since the last backup job. This happens if it is not possible to determine what files have been modified using the NTFS USN Journal. Linux backups are always running in second-pass.

> Note that some firmware upgrades require all data sources protected by the Barracuda Backup Agent to undergo a data verification check on the next scheduled backup. The one-time data verification causes increased backup windows. For this reason, Barracuda recommends upgrading your device firmware over a weekend or during a scheduled maintenance period.



- **Third-Pass Backup** *(Windows only)* – A backup job (or subset of selections within a job) for which the Agent can rely on the NTFS USN Journal to determine which files have been modified since the last backup job. Third-pass backups are only possible on computers running Microsoft Windows. The term is a misnomer since the second backup job run against a Windows machine could be running in third-pass if the NTFS USN Journal is usable.

Security

The Barracuda Backup Agent uses TLS 1.2 (128-bit AES) to both authenticate with a Barracuda Backup device and encrypt the connection between the Barracuda Backup Agent and the Barracuda Backup device.

Authentication

The Barracuda Backup Agent uses public key authentication to verify that it is communicating with a valid Barracuda Backup device. Once communication has been established between the Agent and the Barracuda Backup device, the Agent and Backup device are paired together. This means that the Agent will only successfully communicate with the Backup device with which it is paired. This form of authentication between the Agent and the Barracuda Backup device can help prevent potential man-in-the-middle (MITM) attacks.

In cases where the Agent and Backup device trusted relationship must be broken, such as re-configuring an Agent to backup data to a different Barracuda Backup device, uninstalling and reinstalling the Agent will reset communication. Data can be restored successfully from a Barracuda

Backup device to any Backup Agent that it has a trusted relationship with. If data needs to be restored to an Agent that is currently paired with another Barracuda Backup device, uninstalling and reinstalling the Agent will reset communication.

Encryption

Barracuda leverages the Advanced Encryption Standard-New Instructions (AES-NI) encryption instruction set to perform encryption. AES-NI is used to accelerate data encryption. By default, the Barracuda Backup Agent and the Barracuda Backup device attempt to communicate over the encrypted connection. If AES-NI is supported by the source system where the Agent is installed, as well as the Barracuda Backup device, the data transfer between the Agent and the Barracuda Backup device is encrypted.

If AES-NI is *not* supported by the source system where the Agent is installed or the Barracuda Backup device, the data transfer between the Agent and the Barracuda Backup device is *not* encrypted. The decision to transfer in an unencrypted state is done to prevent slower backup performance on systems not supporting the hardware acceleration that the AES-NI instruction set provides. Encryption of data between the Agent and the Barracuda Backup device can be permanently enabled or disabled by Barracuda Technical Support. If you wish to enable encryption on systems that do not support AES-NI, Barracuda Technical Support can enable encryption, however, backup speeds may be slower than normal.

To help determine if your source system supports encryption, Table 1 lists the processors that support the AES-NI instruction set.

Table 1. Processors Supporting AES-NI Instruction Set.

Source System	Processors

Intel	Westmere based processors, specifically: • Westmere-EP (Xeon 56xx) (a.k.a. Gulftown Xeon 5600-series DP server model) processors • Clarkdale processors (except Core i3, Pentium and Celeron) • Arrandale processors (except Celeron, Pentium, Core i3, Core i5-4XXM) Sandy Bridge processors: • Desktop: all except Pentium, Celeron, Core i3 • Mobile: all Core i7 and Core i5. Several vendors have shipped BIOS configurations with the extension disabled; a BIOS update is required to enable them. Ivy Bridge processors. • All i5, i7, Xeon and i3-2115C only Haswell processors (all except i3-4000m, Pentium and Celeron) Broadwell processors (all except Pentium and Celeron) Silvermont/Airmont processors (all except Bay Trail-D and Bay Trail-M) Goldmont processors Skylake processors Kaby Lake processors Coffee Lake processors
AMD	Jaguar-based processors and newer Puma-based processors and newer "Heavy Equipment" processors • Bulldozer-based processors • Piledriver-based processors • Steamroller-based processors • Excavator-based processors and newer Zen-based processors

Microsoft Windows

The Barracuda Backup Agent for Windows leverages Microsoft VSS and VSS Writers to retrieve information about the files and applications to be backed up, freeze I/O operations, and create and remove shadow copies. The Barracuda Backup Agent protects the Windows File System, System State, and the following Microsoft Applications:

- Microsoft Exchange Server
- Microsoft SQL Server
- Microsoft Hyper-V

Support for Microsoft Exchange Server, Microsoft SQL Server, and Microsoft Hyper-V is embedded in the Barracuda Backup Agent. No application-specific agents are required in addition to the Agent. When configuring a data source, the Barracuda Backup Agent automatically detects the presence of Exchange, SQL, or Hyper-V based on the VSS Writers on the system.

macOS and Linux

The Barracuda Backup Agents for both macOS and Linux protect the file system of the system where they are installed. The Barracuda Backup Agent walks the file system scanning for new, modified, or removed files. While the Agent for macOS and Linux protects all files on the system, bare metal recovery is not supported. The Barracuda Backup Agents for macOS and Linux do not include native application support. In cases where an application is running and needs to be protected, it is advised that the application creates a dump or backup file that the Agent backs up as part of the file system backup.

Resource Consumption

The Barracuda Backup Agent runs as a service on the client system that it is protecting. The resources consumed by the Barracuda Backup Agent on the client system it is installed on are minimal. The amount of memory (RAM) consumed should be no more than 1-2 GB maximum and, in most cases, will never exceed 1 GB.

During a backup window, CPU and disk I/O usage will increase. It is recommended that you schedule backup windows during non-peak hours or during a less busy time for the client system to reduce the impact on normal operations, especially on older systems or systems with heavy I/O usage.

The Barracuda Backup Agent requires some hard disk storage for the tracking database. The size of the database is dependent on the number of files being protected on the client system. As the number of files increases, so does the size of the agent tracking database. Barracuda recommends 1 GB of disk space for every one million files protected.

Creating Pre- or Post-Agent Backup Commands

You can run a pre- or post-Agent backup commands for batch files by editing the **config.ini** file. This enables you to stop and start certain processes on the host computer where the Barracuda Backup Agent is installed. This allows you to stop conflicting processes during the time that the Barracuda Backup Agent is backing up files or create backup dump files prior to backup.

Microsoft Windows

Here is an example of how to edit the Barracuda Backup Agent **config.ini** file to start a process prior to the Barracuda Backup Agent beginning its backup:

1. Navigate to the **config.ini** file on the server in the following location: **C:\Program Files\Barracuda\Barracuda Backup Agent\config**
2. Open the **config.ini** file in a text editor, and in the **[configuration]** section, add the following lines:
   ```
   # the batch file to start the process
   postExecuteScript=c:\start.bat
   ```
3. Save and close the file.

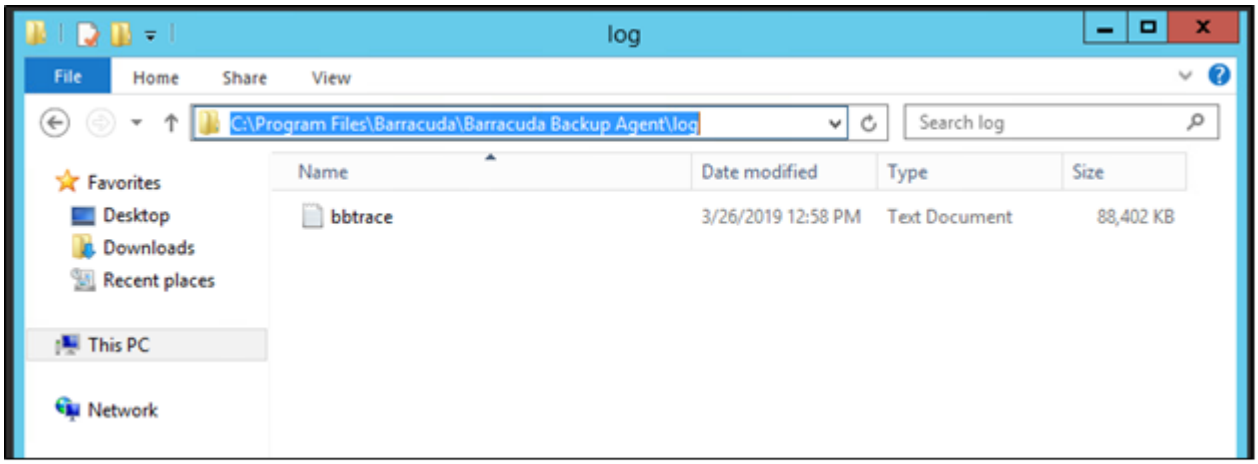
Linux

Here is an example of how to edit the Barracuda Backup Agent **config.ini** file to start a process prior to the Barracuda Backup Agent beginning its backup:

1. Navigate to the **config.ini** file located in **"/usr/local/barracuda/bbs/config/"** on the system where the Barracuda Backup Agent is installed.
2. Open the **config.ini** file in a text editor, and below the **[configuration]** section, enter the following lines:
   ```
   preExecuteScript=/root/script.sh
   postExecuteScript=/root/script.sh
   ```
3. Save and close the file.

Agent Log Files

The Barracuda Backup Agent for Windows, Linux, and MacOS has a log file, `bbtrace.txt`, that can be used for troubleshooting agent backup and recovery errors and warnings. The log file is created by the agent and kept in the agent installation directory, `\Barracuda Backup Agent\log`.



The Barracuda Backup Agent logs are kept as long as the agent or the agent installation folders are not removed. Reinstalling the agent does not remove the `bbtrace.txt` log. The agent logs are not backed up and are automatically excluded by the Barracuda Backup Agent. To keep the logs, or to

make a secondary copy, copy them to a different location from the log folder.

Secondary logs are created on the Barracuda Backup device and are stored indefinitely, or until you wipe the Barracuda Backup device. These logs contain a record of all the processes taking place on the Barracuda Backup device and are used by Barracuda Technical Support for troubleshooting.

Figures

1. source_deduplication.png
2. firstpass.png
3. source_deduplication.png
4. bbtrace.png