Dell EMC DD BoostFS for Windows

Configuration Guide 7.10

Version 7.10

October 2022
Rev. 01

DELL EMC

Notes, cautions, and warnings

NOTE: A NOTE indicates important information that helps you make better use of your product.

CAUTION: A CAUTION indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.

WARNING: A WARNING indicates a potential for property damage, personal injury, or death.

Contents

Figures

Tables

1

Introduction to BoostFS for Windows

Topics:

Revision history

The following table presents the revision history of this document.

Table 1. Revision history of BoostFS for Windows Configuration Guide, version 7.10

Revision	Date	Description
01	October 2022	Initial 7.10 release.

Introduction to BoostFS

DD Boost Filesystem (BoostFS) 7.10 provides a general file-system interface to the DD Boost library, allowing standard backup applications to take advantage of DD Boost features.

Advantages of BoostFS

By leveraging the DD Boost technology, BoostFS helps reduce bandwidth, can improve backup-times, offers load-balancing, allows in-flight encryption, and supports the DD multi-tenancy feature set.

In-flight encryption supported via DDBoost allows applications to encrypt in-flight backup or restore data over LAN from the protection system. When configured, the client is able to use TLS to encrypt the session between the client and the protection system. DD 7.9, 7.8, 7.7, 7.6.0.5, and later versions support GCM based ciphers in both Boost client and DD. Details can be found in the *DD Boost for OpenStorage Administration Guide*, *DD Boost Partner Integration Guide*, *DD Boost SDK Programmers Guide*, and *DD Security Configuration Guide*.

As a file server system implementation, the BoostFS workflow is similar to CIFS but also leverages the DD Boost protocol. In addition, BoostFS improves backup times compared to CIFS and various copy-based solutions.

BoostFS supports single-node Data systems, high-availability (HA) systems, DD Virtual Edition, and Extended Distance Protection.

Purpose

This document describes how to install and configure BoostFS on client systems.

Supported environments

Environments that use BoostFS 7.10 must meet the following specifications.

BoostFS for Windows requires the following:

- DD OS version 6.1.2 or later

- Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, or Windows Server 2019

Supported applications

The Dell EMC DD BoostFS support matrix, available from E-Lab Navigator at https://elabnavigator.emc.com/eln/elnhome, lists the supported applications. From the E-Lab Nabigator home page, select **Data Protection And Availability Solutions** > **PowerProtect DD series appliances**.

Boost features supported by BoostFS

Transport Layer Security (TLS) anonymous authentication is supported to provide encryption.

NOTE: If you select TLS, be aware that there is no configuration option to enable TLS from the client. It must be enabled through the PowerProtect or Data Domain System.

Boost features not supported by BoostFS

- Managed File Replication (MFR)
- DD Boost-over-Fibre Channel (DFC)
- Retention Lock

Compatibility

BoostFS for Windows does not support accessing files and directories that are created by other means, such as BoostFS for Linux, other Boost-enabled applications, NFS, or CIFS.

If you use ACL functionality with BoostFS for Windows, changing file permissions by a protocol other than BoostFS for Windows causes the ACLs to be lost.

Unsupported file system features

BoostFS for Windows does not support the following NTFS features through the file system interface:

- Alternate data streams
- File links
- Quotas

2

Preparing the PowerProtect or Data Domain system for BoostFS

Topics:

Prepare the system for BoostFS

Every system that is enabled for DD Boost deduplication must have a unique name. You can use the system DNS name, which is always unique.

Prerequisites

Ensure that all your systems can access the Key Distribution Center (KDC). In a Windows environment, the Windows server that hosts the Microsoft Active Directory service acts as the KDC and the domain name system (DNS). If the systems cannot reach the KDC, check the DNS settings at `/etc/resolv.conf`.

Steps

1. On the PowerProtect or Data Domain system, log in as an administrative user.
2. Verify that the file system is enabled and running by entering:

```
$ filesys status
The file system is enabled and running.
```

3. Verify that DD Boost is already enabled:

```
$ ddboost status
DD Boost status: enabled
```

If the DD Boost status is reported as disabled, enable it by entering:

```
$ ddboost enable
DD Boost enabled
```

4. Verify that distributed segment processing is enabled:

```
ddboost option show
```

You should see the following output:

```
Option                                Value
-----------------------------------   --------
distributed-segment-processing        enabled
virtual-synthetics                    enabled
fc                                    disabled
global-authentication-mode            none
```

```
global-encryption-mode                  medium
----------------------------------   ---------
```

If distributed segment processing is shown as disabled, enable it by entering:

```
ddboost option set distributed-segment-processing enabled
```

NOTE:

- If secure multi-tenancy (SMT) is used, the user role must be set as `none`.
- Users who run backup applications that connect to Power Protect or Data Domain systems must have their user names configured on that system. For more information, see the *DD OS Administration Guide*.
- Multiple applications can use DD Boost to access a Power Protect or Data Domain system, and multiple users can be configured for DD Boost access. The username, password, and role must have already been set up using the DD OS `user add` command:

```
user add <user> [password <password>]
[role {admin | limited-admin | security | user | backup-operator | data-access}]
[min-days-between-change <days>] [max-days-between-change <days>]
[warn-days-before-expire <days>] [disable-days-after-expire <days>]
[disable-date <date>] [force-password-change {yes | no}]
```

For example, to add a user with a login name of **`jsmith`** and a password of **`mP34$muk*E`** with administrative privilege, enter:

```
$ user add jsmith password mP34$muk*E role admin
```

Once the user has been created, the user must be made a DD Boost user. To add **`jsmith`** to the DD Boost user list, enter:

```
$ ddboost user assign jsmith
```

Set the system hostname and domain name

Set the system host name and the domain name in DD OS using the **`net set`** CLI command.

Steps

In DD OS, type the following:

```
# net set hostname [host]
# net set {domain name [local-domain-name]}
```

For more information on **`net`** commands, see the *DD OS Command Reference Guide*.

Prepare the system for Kerberos authentication

Join a PowerProtect or Data Domain system to an Active Directory domain

About this task

Joining the system to an Active Directory domain is required for access control list (ACL) support and Kerberos authentication. If you do not plan to use ACLs or Kerberos in your implementation, this procedure is not required.

For more information about ACLs, see File security on page 26. For more information about Kerberos authentication, see Configure the BoostFS client for Kerberos authentication on page 20.

Steps

1. To join a system to an Active Directory domain, type the following command:

   ```
   # authentication kerberos set realm <domain> kdc-type windows
   ```

   You are prompted to type credentials for the domain.
2. Type the domain username and password.

Results

If the credentials are valid, the system is joined to the Active Directory domain. The use of this command does not enable CIFS.

BoostFS and existing DD OS commands

You must create one or more storage units on each PowerProtect or Data Domain system enabled for BoostFS. System administrators can use existing DD OS CLI commands to create and manage storage units used by BoostFS.

Assign multiple users to BoostFS

When, as a system administrator, you create the storage units that users employ with the backup applications, you associate a username with each storage unit. This associated username can be changed after creation of the storage unit.

Storage units are accessible only to applications with the username that owns the storage unit.

Each storage unit is owned by one username, and the same username can own multiple storage units. The application passes the username and password to BoostFS, and DD Boost passes them to the PowerProtect or Data Domain system when attempting to connect to the system. The system then authenticates the username and password. The username and password can be shared by different applications.

When a storage unit is created with a valid local user but not assigned to DD Boost, the user is automatically added to the DD Boost users list in the same way that a user is added via the `ddboost user assign` command.

Assign one or more users to the DD Boost users list:

```
$ ddboost user assign user1 user2
User "user1" assigned to DD Boost.
User "user2" assigned to DD Boost.
```

To verify and display the users in the users list, enter:

```
$ ddboost user show

DD Boost user   Default tenant-unit   Using Token Access
-------------   -------------------   ------------------
user1           Unknown               Yes
user2           Unknown               -
user3           Unknown               Yes
user4           Unknown               -
user5           Unknown               -
user6           Unknown               -
user7           Unknown               Yes
user8           Unknown               -
-------------   -------------------   ------------
```

To unassign the user from the users list, enter:

```
$ ddboost user unassign user1
User "user1" unassigned from DD Boost.
```

Create storage units

You need to create one or more storage units on each PowerProtect or Data Domain system enabled for BoostFS.

Steps

1. Create a storage unit in DDOS:

   ```
   $ ddboost storage-unit create NEW_STU1 user user1
   Created storage-unit "NEW_STU1" for "user1".
   ```

   A storage unit name must be unique on any given PowerProtect or Data Domain system. However, the same storage unit name can be used on different systems.

   The username owns the storage unit and ensures that only connections with this username's credentials are able to access this storage unit. See the section on ddboost storage-unit commands in the *DD OS Command Reference Guide* for details on command options.

2. Repeat the previous step for each storage-unit needed in DD OS.
3. If you want to modify a DD OS storage unit, enter:

   ```
   $ ddboost storage-unit modify NEW_STU1 user user2
   Storage-unit "NEW_STU1" modified for user "user2".
   ```

   The `ddboost storage-unit modify` command allows the backup application to change the username ownership of the storage unit. Changing the username does not require that attributes of every file on the storage unit be changed.

4. Display the users list for the storage units:

   ```
   $ ddboost storage-unit show
   ```

   After entering the command, the output you see should be similar to the following:

```
# ddboost storage-unit show
Name                 Pre-Comp (GiB)   Status   User        Report Physical
                                                              Size (MiB)
-----------------    --------------   ------   --------    ---------------
backup                          3.0       RW   sysadmin                  -
DDBOOST_STRESS_SU              60.0       RW   sysadmin                  -
task2                           0.0       RW   sysadmin                  -
tasking1                        0.0       RW   sysadmin                  -
DD1                             0.0       RW   sysadmin                  -
D6                              5.0       RW   sysadmin                  -
TEST_DEST                       0.0       D    sysadmin                  -
STU-NEW                         0.0       D    ddul                      -
getevent                        0.0       RW   ddul                      -
DDP-5-7                       120.0       RW   sysadmin                  -
TESTME                        150.0       RW   sysadmin                  -
DDP-5-7-F                     100.0       RW   sysadmin                  -
testSU                          0.0       RW   sysadmin                200
-----------------    --------------   ------   --------    ---------------
D    : Deleted
Q    : Quota Defined
RO   : Read Only
RW   : Read Write
RD   : Replication Destination
```

Next steps

If you are using Kerberos authentication in your implementation, you must create an Active Directory user with the same name as the storage-unit user.

Logical stream limits for storage units (optional)

BoostFS is restricted to the same stream limit and storage quota features as DD Boost. See the *DD Boost for Partner Integration Administration Guide* for more information.

Client Groups and BoostFS

The Client Group feature identifies specific client loads when clients are associated with groups.

The `client group` command set is supported only for clients that use DD Boost or NFS protocols. For more information about Client Groups, see the *DD OS Command Reference Guide*.

Distributed segment processing option

BoostFS supports distributed segment processing as supported by DD Boost. For more information, refer to the *DD OS Administration Guide*.

NOTE: Enabling or disabling the distributed segment processing option does not require a file system restart.

3

Installing BoostFS for Windows

Topics:

Installation overview

Install or upgrade BoostFS for Windows by using the provided MSI installer. Do not change the default settings.

NOTE: If you are prompted to restart after installing, failure to do so can cause features such as Explorer integration to not work correctly. If you are not prompted to restart, restarting is not necessary.

Prerequisites

When installing or upgrading BoostFS for Windows:

- Use an account with administrator rights to run the installer.
- Ensure that there is enough free space to complete the installation, which requires approximately 7 MB of disk space.
- Deactivate all BoostFS mount points. If any mount points are active, the upgrade and removal processes fail.

CBFS driver

The MSI installer includes several binary files as well as a device driver from EldoS Corporation.

BoostFS for Windows uses CBFS, a software interface from EldoS that enables file systems to exist in user space and not only within a driver in kernel space. This functionality is similar to that of FUSE on UNIX operating systems. To install BoostFS for Windows, you must install the CBFS driver from EldoS Corporation.

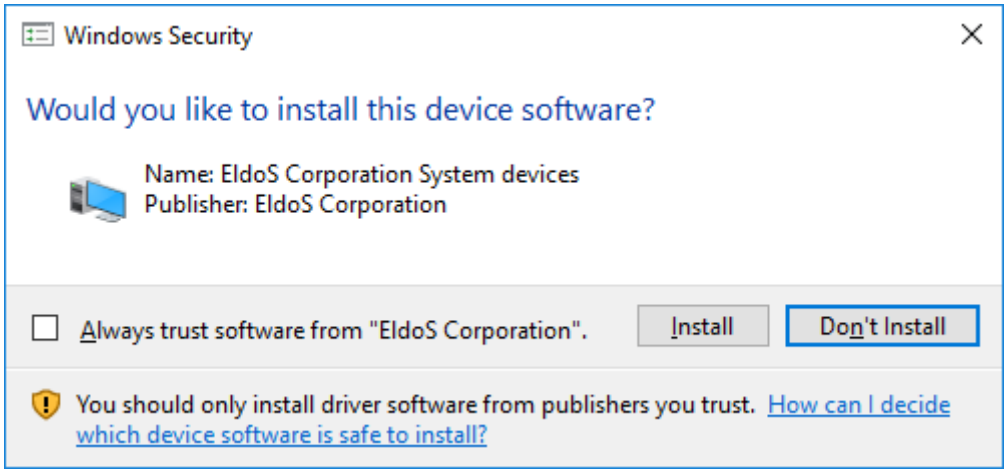

Figure 1. Windows Security warning for the EldoS Corporation device driver

If another program on the system previously installed the CBFS driver, the driver that BoostFS installs is installed alongside it and does not affect operation of the other program.

Components of BoostFS for Windows

Components in the installation location

The BoostFS for Windows installation includes the following files at the installed location:

- `boostfs.exe`—An executable that supports various commands including establishing a BoostFS mount.
- Shared libraries that enable `boostfs.exe`.
- The RSA Lockbox libraries.
- The Universal C Runtime Library (UCRT). If the UCRT is already installed on the system, `boostfs.exe` uses the system version of the UCRT.
- HTML files that provide basic guidance on the use and configuration of `boostfs.exe`.
- If not already installed, the 2012 and 2015 Visual C++ redistributables are installed.

Entries on the **Start Menu**

Three links are added to the **Start Menu** under **Programs** > **BoostFS**.

These links open:

- A command prompt at the installed location of BoostFS.
- The BoostFS help file.
- The BoostFS configuration help file.

Files in `C:\BoostFS`

A directory is created at `C:\BoostFS`. This directory is the default location for BoostFS logs, Lockbox containers, and the sole location of the configuration file `C:\BoostFS\boostfs.conf`. The `Lockbox` and `Logs` directories may be configured to be placed elsewhere after installation, but the configuration file must exist in this location.

A sample configuration file, `C:\BoostFS\boostfs_sample.conf`, is provided.

Upgrade the BoostFS client

To upgrade BoostFS, run the MSI installer of the new BoostFS release.

About this task

NOTE: If you are prompted to restart after upgrading, failure to do so can cause features such as Explorer integration to not work correctly. If you are not prompted to restart, restarting is not necessary.

Uninstall the BoostFS client

About this task

To uninstall BoostFS for Windows, use either of the following methods:

- Run the MSI installer and select **Remove**.
- Use the **Add or remove programs** interface in the **Control Panel**.

4

Configuring and using BoostFS for Windows

Topics:

BoostFS for Windows configuration overview

Specify BoostFS configuration parameters by using the command line interface (CLI), the configuration file, or both.

The BoostFS configuration file location is `C:\BoostFS\boostfs.conf`.

The configuration file has sections for global and mount-point–specific parameters. Mount-point–specific parameter values override global parameter values. If the global section does not define `data-domain-system` and `storage-unit` parameters, those parameters must be passed to the `mount` command by using the CLI.

Parameters that are configured by using the CLI override conflicting values in the configuration file.

The following is a sample configuration file:

```
##############################################################################
# BoostFS example config file for Windows
#
# The configuration file is divided into sections, delineated by brackets [].
# Options that are to apply to all mount points are in the [global] section.
# More details on the various configuration options can be found in the
# BoostFS manual. Command line options override what is in this file.
#
# Format:
# # - Identifies a comment line, and must be at the start. Configuration
# parameters can be disabled by adding a "#" to the start of the line.
#
# Values which contains spaces should use double quotations around the
# entire value.
#
# No whitespace is allowed between the option and the value, i.e.
# log-dir = \path is not allowed.
#
# Comments are not allowed after the option value pair.
#
##############################################################################

[global]
# Data Domain Hostname or IP address
# data-domain-system=dd2500-1.yourdomain.com

# Storage Unit
# storage-unit=su-name

# Security option used for authentication (default: lockbox)
# security=<krb5|lockbox>

# Storage Unit Username (should only be used in conjunction with Kerberos authentication)
# storage-unit-username=sysadmin
```

```
# Lockbox path (default: C:\BoostFS\Lockbox\boostfs.lockbox)
# lockbox-path=C:\lockbox-name

# Enable logging (default: true)
# log-enabled=<true|false>

# Log level (default: info)
# log-level=<debug|info|warning|error>

# Directory for log files (default: C:\BoostFS\Logs)
# log-dir=C:\directory-name

# Log file name (default: ddboostfs_ddr-name_su-name.log)
# A unique log file name should be used for each mount point.
# log-file=unique-file-name.log

# Maximum log size in MB (default: 100MB)
# log-maxsize=100

# Number of log files to save (default: 8)
# log-rotate-num=10

# Text string that describes the application using boostfs with additional information
such as the version.
# app-info="text_string"

# Maximum number of connections that can be used at the same time (default: 128)
# Min value is 64. Max value is 256.
# max-connections=128

# Enable compressed restoration (default: false).
# When set to true, the server conducts data compression before sending to the client.
# Correspondingly, when the client receives data, it needs to conduct decompression first.
# By sending compressed data over the network, bandwidth usage can be reduced. However,
# use this option with caution since it requires significant amount of CPU power to conduct
# compression on the server and to conduct decompression on the client.
# ddboost-read-compression=<true|false>

# Allow for Windows ACLs to be set on files in the mountpoint
# NOTE: Unless the client is joined to an AD domain, this parameter cannot be set to true.
#       When using Kerberos, this parameter value is ignored.
# local-user-security=<true|false> (default: false)

# Expose the mount to user sessions other than the user session in which the mount was
established
# allow-others=<true|false> (default: true)

# Automatically renew Kerberos tickets when Kerberos authentication is used (default: true)
# krb-auto-renew=<true|false>

# UNC Mount point sections are delineated by [UNC Path]
# The UNC Path must be of the form [\\ddr-name\su-name].
# Forward slashes and extra slashes must not be used.

# [\\ddr-name\su-name]
# Drive Letter specifies the Windows drive to map to this UNC mount point
# drive-letter=h:
```

BoostFS for Windows command overview

Use the Windows command prompt or PowerShell to issue BoostFS commands.

The BoostFS installation includes a shortcut on the Start menu to open the command prompt in the directory containing the executable. During the installation process, the installer can automatically add the location of the executable to the *PATH* environment variable so that you do not need to specify the path when issuing BoostFS commands. If you do not choose this option during installation, you can add the location manually later.

For detailed information about a BoostFS command, see the corresponding section in the HTML help file.

BoostFS parameters

The following parameters are used to configure BoostFS:

<data-domain-system>	The hostname or IP address of the PowerProtect or Data Domain system.
<storage-unit>	The target storage unit on the PowerProtect or Data Domain system.
<storage-unit-username>	The username of the storage unit owner on the PowerProtect or Data Domain system.
<lockbox-path>	The path to the lockbox file. If this parameter is not set with the CLI or in the configuration file, the default path is `C:\BoostFS\Lockbox\boostfs.lockbox`.
<UNC-mount-path>	The Universal Naming Convention (UNC) path of the mounted storage-unit. The UNC path must be of the form `\\<data-domain-system>\<storage-unit>`
<drive-letter>	The drive letter to which the BoostFS mount is mapped.

BoostFS and high availability

If you are configuring a high availability (HA) system, you should make sure the IP address (or hostname) that you specify for the system is one of the floating IP addresses. Only the floating IP addresses in an HA system are accessible after a failover.

If you incorrectly specify one of the fixed HA addresses, you will not be able to connect to the PowerProtect or Data Domain system in the event of a recoverable failure.

Authentication methods

BoostFS has two authentication options:

- RSA Lockbox
- Kerberos

RSA Lockbox-based authentication

RSA Lockbox is the default password manager for BoostFS for Windows.

To use RSA Lockbox, you need to set the lockbox using the `boostfs lockbox set` command. You can also set up a shared BoostFS lockbox file.

Sharing a BoostFS Lockbox file on multiple clients

Sharing a common Lockbox file enables you to create a single management point for BoostFS clients to access BoostFS mount points on PowerProtect or Data Domain systems.

You can create a common Lockbox file for all BoostFS clients from a primary client. This feature allows you to avoid creating a separate Lockbox file for each unique BoostFS client.

The primary client is the client from which the shared Lockbox is initially created. Since some operations can only be performed from the primary client, it is recommended to record which client is the primary.

The easiest way to share a Lockbox file is to store it in a network share that is accessible by all clients that use it.

Create the Lockbox on the primary client

Prerequisites

Verify that BoostFS is installed on the server that manages access to the shared Lockbox.

NOTE: The command `boostfs lockbox set` fails if there is an existing Lockbox file in the same location.

About this task

In this example, `Z:\` represents the network share that is accessible by all clients.

Steps

1. Create the Lockbox with the `-l` option:

   ```
   boostfs lockbox set -u <storage-unit-username> -d <data-domain-system> -s <storage-unit>
   -l Z:\boostfs.lockbox
   ```

   You can also specify the *lockbox-path* in the configuration file.
2. Repeat the `lockbox set` command for each PowerProtect or Data Domain system or storage unit that needs to be accessed by the Lockbox.

Use the shared Lockbox on other clients

Prerequisites

Create a shared Lockbox and add credentials for the PowerProtect or Data Domain systems and storage units that need access to the Lockbox.

About this task

In this example, `Z:\` represents the network share that is accessible by all clients.

Steps

1. To allow access to the Lockbox for the other clients, type the following command on the primary client:

   ```
   boostfs lockbox add-hosts -l Z:\boostfs.lockbox client1.dell.comclient2.dell.com
   ```

   In this example, clients with the hostname ***client1.dell.com*** and ***client2.dell.com*** are allowed access to the shared Lockbox.
2. On each client that needs access to the shared Lockbox, specify the path to the shared Lockbox by either:
   - Using the `mount` command:

     ```
     boostfs mount -d <data-domain-system> -s <storage-unit> -l Z:\boostfs.lockbox
     ```
   - Editing the configuration file:

     ```
     [global]
     lockbox-path=Z:\boostfs.lockbox
     ```

View clients accessing the shared lockbox

About this task

Clients allowed to access the lockbox can be viewed by using lockbox `show-hosts` command as below:

```
/boostfs lockbox show-hosts -l /mnt/nfsshare/boostfs.lockbox
```

In this example the output will be:

```
./boostfs lockbox show-hosts -l /mnt/nfsshare/boostfs.lockbox
Security Access List:
        client1.dell.com
        client2.dell.com
```

Modify the shared Lockbox

About this task

Only the primary client can modify the Lockbox file. Other clients encounter an error when they try to modify the Lockbox. Other clients are still able to query the Lockbox.

In this example, `Z:\` represents the network share that is accessible by all clients.

Steps

1. To remove client access:

   ```
   boostfs lockbox delete-hosts -l Z:\boostfs.lockbox client2.dell.com
   ```

   NOTE: After removing a client from the Lockbox, the client can no longer use the Lockbox and can no longer access any of the PowerProtect or Data Domain systems defined in the Lockbox.

2. To remove a Lockbox entry:

   ```
   boostfs lockbox remove -d <data-domain-system> -s <storage-unit> -l Z:\boostfs.lockbox
   ```

   NOTE:

   After removing a PowerProtect or Data Domain system or storage unit from those that the Lockbox grants access to, none of the clients that use the Lockbox can access the system or storage unit.

Kerberos-based authentication

BoostFS Windows supports the MIT implementation of Kerberos authentication as an alternative to RSA lockbox authentication.

There are three main entities involved with Kerberos Authentication:

- BoostFS client
- An Active Directory server acting as the Kerberos Key Distribution Center (KDC)
- PowerProtect or Data Domain system running DD OS version 6.0 or later

The Kerberos file contains a "shared secret" (a password, pass phrase, or other unique identifier) between the KDC server and the PowerProtect or Data Domain system.

In an Active Directory environment, the Windows server that hosts the Active Directory service also acts as the Key Distribution Center (KDC) and also a domain name system (DNS).

Kerberos tickets

To authenticate using Kerberos, you must acquire a Ticket Granting Ticket (TGT) for two types of user accounts:

- A Kerberos Ticket Granting Ticket (TGT)
- A Kerberos ticket for various services (service tickets) that the client will use (BoostFS, DNS, CIFS, NFS, etc.)

Each user only has access to the tickets they create with the BoostFS Kerberos commands. Users cannot access tickets that others have created.

For more detailed information about using Kerberos with BoostFS, see Considerations for Kerberos authentication on page 22.

Configure the BoostFS client for Kerberos authentication

Kerberos authentication uses tickets to authenticate instead of a username and password.

Prerequisites

Verify that each of the following requirements are met:

- The PowerProtect or Data Domain system and the client resolve DNS for each other.
- The client is joined to the same Active Directory domain as the PowerProtect or Data Domain system.

- The PowerProtect or Data Domain system, client, and Active Directory server system clocks must be within five minutes of each other. Using an NTP server is a reliable way to keep the clocks synchronized.
- There must be a user in the Kerberos realm with the same name as the storage-unit user local to the PowerProtect or Data Domain system. You must use the Kerberos realm credentials to acquire the storage-unit user ticket, not the credentials local to the PowerProtect or Data Domain system.

Steps

1. Acquire a storage-unit user TGT.

   This TGT grants access to the mount point and is required to mount BoostFS. For more information, see Acquire the storage-unit user ticket on page 21.
2. Mount BoostFS as the storage-unit user.

   For more information, see Mount BoostFS on page 21.
3. Acquire a primary Kerberos user TGT.

   This TGT determines access to files and directories within the mount point. Each user that requires file access after mounting BoostFS must have a primary user ticket. For more information, see Acquire the primary user ticket on page 22.

Acquire the storage-unit user ticket

The storage-unit user TGT grants access to the mount point and is required to mount BoostFS.

Prerequisites

Review the prerequisites in Configure the BoostFS client for Kerberos authentication on page 20.

Steps

1. To create a storage-unit user ticket, use the `kerberos set` command with the `-u` option and specify the storage-unit username:

   ```
   # boostfs kerberos set -u <storage-unit-username>
   ```

   NOTE:
   - You must use the Kerberos realm credentials to acquire the storage-unit user ticket, not the credentials local to the PowerProtect or Data Domain system.
   - To allow other users on the client system to mount BoostFS, include the option **`-o allow-others=true`**. This option can only be changed by an administrator.
2. (Optional) To verify the creation of the storage-unit user ticket, use the `-u` option and specify the storage-unit username:

   ```
   # boostfs kerberos query -u <storage-unit-username>
   ```

Mount BoostFS

About this task

For more information about mounting BoostFS, see Considerations for Kerberos authentication on page 22 and Mounting the BoostFS file system on page 23.

Steps

Mount BoostFS and specify Kerberos authentication:

```
boostfs mount -d <data-domain-system> -s <storage-unit> -o security=krb5 -o <storage-unit-username=mount-point>
```

Results

BoostFS is mounted, but inaccessible.

Acquire the primary user ticket

Steps

1. To create a primary Kerberos user ticket, use the `-m` option and specify the primary Kerberos username:

   ```
   # boostfs kerberos set -m <primary-username>
   ```

2. (Optional) To verify the creation of a primary Kerberos user ticket, use the `-m` option without specifying a username:

   ```
   # boostfs kerberos query
   ```

Results

The client configuration is complete.

Considerations for Kerberos authentication

Kerberos implementation

BoostFS uses MIT Kerberos, which has a separate configuration file located at `C:\ProgramData\MIT\Kerberos5\krb5.ini`. This configuration file can be used to control ticket lifetime and make other changes to the Kerberos implementation. For additional information about changing the Kerberos configuration, and other information not specific to the BoostFS implementation, refer to MIT Kerberos documentation.

The credential for the storage-unit user is stored in `C:\BoostFS\Kerberos\<process-username>\<storage-unit-username>`. The credential for the primary Kerberos user is stored in `C:\BoostFS\Kerberos\<process-username>\<primary-username>`.

Security and file permissions

When using Kerberos for authentication, ACL support is automatically enabled. Setting system ACLs is not supported.

To allow other users on the client system to mount BoostFS, include the option `-o allow-others=true` when using `boostfs kerberos set -u <storage-unit-username>`. When this option is used, the storage-unit user ticket is shared with any user of the mount point. However, other users must still have their own primary user ticket to access the files and directories within the mount. This option can only be changed by an administrator.

By default, the `local-user-security` parameter is set to `false`. When using RSA Lockbox authentication, this setting can be changed to `true`. When using Kerberos authentication it is always set to `true` and ignores any conflicting options in the configuration file.

Any files created through the primary Kerberos user's connection to the BoostFS mount are owned by that primary user. These files can only be changed by a user with the same TGT.

You can optionally configure the client access list for DD Boost on the PowerProtect or Data Domain system to only use Kerberos authentication by typing the following command on the system: `# ddboost client add <client-name> authentication-mode kerberos`

NOTE: If you perform this optional step, note that a BoostFS client configured to use Kerberos must use Kerberos for the connection to succeed. If that BoostFS client uses RSA Lockbox, the connection will fail.

Renewing tickets

When the `krb-auto-renew` option is used, tickets are automatically renewed up to their renewable time. Once the renewable time has been exceeded, you must manually acquire the ticket again using the BoostFS Kerberos commands.

Mounting the BoostFS file system

To allow BoostFS mount on the DD System, NFS version 3 must first be enabled. BoostFS uses the NFSv3 service internally to interact with the DD system. Use the commands given.

- To enable NFSv3: `nfs enable version 3`
- To verify if NFSv3 is enabled or not: `nfs status`

The `boostfs mount` command allows you to mount the BoostFS file system. You can mount the BoostFS file system in either of the following two ways:

- To use a UNC mount path, type:

  ```
  boostfs mount [-l <lockbox-path>] [[-o <param>=<value>] ...] <UNC-mount-path> [<drive-letter>]
  ```

  Where the UNC mount path is in the form `\\<data-domain-system>\<storage-unit>`.
- To use the PowerProtect or Data Domain system and storage unit names, type:

  ```
  boostfs mount -d <data-domain-system> -s <storage-unit> -o security=kerb5 -u <storage-unit-username> <mount-point>
  ```

  Where `-d` specifies the system and `-s` specifies the storage unit.

If no drive letter is specified, the mount is only accessible through the UNC path.

If a BoostFS mount is established with an optional drive letter, the drive letter must be an unused drive letter. On mount, the drive shows up in the Windows Explorer sidebar immediately.

After mounting without a drive letter, you can use the **Map Network Drive** context option in Explorer or the `net use` command to map the UNC path to a drive letter.

NOTE: BoostFS does not support files being executed on the mount point.

Command options for boostfs mount

The following options are valid for the `boostfs mount` command.

Table 2. Command options for `boostfs mount`

Option	Description
`-o allow-others=<true | false>`	Allow users on the client system other than the owner of the mount to mount BoostFS. Default value: `false` For more information, see Considerations for Kerberos authentication on page 22
`-o app-info="text_string"`	Display a text string describing the application using BoostFS.
`-o data-cache=<enable|disable>`	Option to enable data-cache which results in performance improvement for MSSQL multi-streams environment. Default value: disable
`-o ddboost-read-compression=<true | false>`	Enable compressed restoration. Default value: `false` For more information, see Compressed restoration on page 25
`-o krb-auto-renew=<true | false>`	Allow tickets to be automatically renewed up to their renewable time. Once the renewable time is exceeded, you must manually acquire the ticket again using the BoostFS Kerberos commands. Default value: `false`

Table 2. Command options for `boostfs mount` (continued)

Option	Description
`-o local-user-security=<true | false>`	Allow Windows ACLs to be set on files in the mount point. Default value: `false` For more information, see File security on page 26.
`-o log-enabled=<true | false>`	Enable or disable logging. Default value: `true`
`-o log-level=<debug | info | warning | error>`	Set the log detail level. Default value: `info`
`-o log-dir=C:\directory-name`	Specify the directory for log files. Default value: `C:\BoostFS\Logs`
`-o log-file=unique-file-name.log`	Specify the log file name. Default value: `ddboostfs_ddr-name_su-name.log`
`-o log-maxsize=100`	Specify the maximum log size in MB. Default value: `100`
`-o log-rotate-num=8`	Specify the number of log files to save. Default value: `8`
`-o max-connections=128`	Specify the maximum number of connections that can be used at the same time. Default value: `128` For more information, see Maximum connections for boostfs mount on page 25.
`-o security=<krb5 | lockbox>`	Specify the security option used for authentication Default value: `lockbox`
`-o storage-unit-username=sysadmin`	Specify the storage unit user name. Use only with Kerberos.

Mount on startup

BoostFS is a regular process that the operating system stops when the system restarts or the user logs off, and BoostFS for Windows mounts do not survive without the process.

To remount BoostFS mounts during system startup, you can add `boostfs mount` commands as part of a system startup or user login script. For information on system startup and user login scripts, refer to Microsoft documentation.

BoostFS client connection details

After mount points are created, you can use the `ddboost show connections` command to see details about clients that use BoostFS to connect to the PowerProtect or Data Domain system.

The details displayed in the output include the BoostFS version number and the Boost library, as shown in the following example:

```
dduser@ddve1# ddboost show connections

Active Clients: 0

Clients:
Client                  Idle  Plugin Version  OS Version                                  Application Version                                  Encrypted  DSP  Transport
----------------------  ----  --------------  ------------------------------------------  ---------------------------------------------------  ---------  ---  ---------
client.yourdomain.com   YES   3.4.2.0-593989  Microsoft Windows Server 2012, 64-bit       BOOSTFS:1.2.0.1-594272 ucsload05 CBFS 6.1            NO         YES  IPv4
----------------------  ----  --------------  ------------------------------------------  ---------------------------------------------------  ---------  ---  ---------

Client Connections:
Max Client Connections: 180
---------- ifgroup ----------  ---------- Client Connections ----------  - DD Connections -  --------
                               ------- Control -------  --------- Data ---------
Group-name  Status  Interface                          Write  Read  Src-repl  Dst-repl  Synthetic  Repl-out  Repl-in  Total
----------  ------  ---------------------------------  -----  ----  --------  --------  ---------  --------  -------  -----
none                                      10.6.109.148      0     0         0         0          0         0        0      0
none                2620:0:170:1604:2a0:d1ff:feec:d071      0     0         0         0          0         0        0      0
----------  ------  ---------------------------------  -----  ----  --------  --------  ---------  --------  -------  -----
                                     Total Connections:      0     0         0         0          0         0        0      0
----------  ------  ---------------------------------  -----  ----  --------  --------  ---------  --------  -------  -----
```

Figure 2. `ddboost show connections` display

See the *DD OS Command Reference Guide* for more information about the `ddboost show connections` command.

Compressed restoration

This option reduces bandwidth usage when sending and receiving data, but increases CPU usage.

When the mount option `ddboost-read-compression` is set to `true`, data is compressed on the server before being sent to the client. When the client receives the data, it must decompress the data. Sending and receiving compressed data uses less network bandwidth, but compressing and decompressing the data requires a significant amount of CPU power. By default, this option is set to `false`.

This option can be used in one of the following two ways:

- As a command-line option:

  ```
  boostfs mount -o ddboost-read-compression=true /mnt/bfs-mount
  ```
- As an option configured in the `boostfs.conf` file:

  ```
  ddboost-read-compression=true
  ```

Maximum connections for boostfs mount

You can use the `max-connections` mount option to specify the maximum number of simultaneous open files on the BoostFS mount point. The default value is 128, and the value can be set to any value between 64 and 256.

NOTE: Increasing the number of simultaneous open files increase the amount of memory BoostFS uses.

Unmounting the BoostFS file system

The `boostfs umount` command allows you to unmount the BoostFS file system.

Use one of the following two formats:

- `boostfs umount <UNC-mount-path>`
- `boostfs umount <drive-letter>`

If the BoostFS file system is mounted with a drive letter, you must unmount by using the drive letter.

If the BoostFS file system is mounted with a drive letter and a mount path, you must unmount by using the drive letter.

If the BoostFS file system is mounted without a drive letter, you must unmount by using the UNC mount path.

If the BoostFS file system is mounted using the Map Network Drive option:

1. Disconnect the network drive.

2. Unmount by using the UNC mount path. Do not use the drive letter.

NOTE: Do not use the Explorer disconnect utility to disconnect a drive that was mapped to a drive letter with the `boostfs mount` command.

File security

If the required conditions are met, BoostFS for Windows supports access control lists (ACLs) on files and directories within the BoostFS mount point.

NOTE: If ACLs are not used, the Boost user credentials are used for all users who access the client mount point. Any files or directories that are created in the mount point are fully accessible by any user with access to the mount point or storage unit.

ACL requirements

- The PowerProtect or Data Domain system and the client must be joined to the same Active Directory domain. If the client is not joined to a domain, ACLs cannot be enabled during the mount process. If the system is not joined to the domain and ACLs are enabled during the mount process, the mount point is not accessible.
- The `local-user-security` option must be set to `true` during mount. This setting can be applied by using the CLI or the BoostFS configuration file.

User identity

When `local-user-security` is enabled, the identity of the client user determines access to a file or directory, not the identity of the storage unit user.

For a user on the client system to access a file in a BoostFS mount point, the ACL on the file must give that user the required rights. Without Active Directory support for ACL configuration, a client user on one system may appear to be a different user when using a different system and be denied access to the file.

With Kerberos, authentication only uses the primary user name and primary user group. Non-primary groups are not supported. Additionally, privileges are not supported, and therefore SACL management is not supported.

ACL default permissions

CAUTION: If you use ACL functionality with BoostFS for Windows, changing file permissions by a protocol other than BoostFS for Windows causes the ACLs to be lost.

File

If no inheritance occurs, the default ACL on a file contains:

- No system access control list (SACL)
- A discretionary access control list (DACL) with the following permissions:

  Creator of the file—Full control
  Group of the creator of the file—Read and execute permissions
  Everyone—Read and execute permissions

If inheritance occurs, the ACL on a file contains the permissions inherited from the parent directory.

Directory

If no inheritance occurs, the default ACL on a directory contains:

- No SACL
- A DACL with the following permissions:

Creator of the directory—Full control on the directory
Group of the creator of the file—Read and execute permissions on the directory
Everyone—Read and execute permissions on the directory

If inheritance occurs, the ACL on a directory contains the permissions inherited from the parent directory.

Subdirectory

Subdirectories and files within the directory inherit the following permissions:

Creator of the subdirectory—Full control
Creator of the file—Full control
Group of the creator of the subdirectory or file—Read and execute permissions
Everyone—Read and execute permissions

5

Troubleshooting

Topics:

Log information

You can use the following log files to diagnose BoostFS problems:

- BoostFS log file

  By default, the BoostFS log file is found the directory `C:\BoostFS\Logs`. The default name of the file is `ddboostfs_<data-domain-hostname>_<storage-unit>.log`, where:

  - `<data-domain-hostname>` is the hostname or IP address for the BoostFS mount
  - `<storage-unit>` is the storage-unit name of the BoostFS mount

  A typical BoostFS log message appears in the following format:

  ```
  Date + Time + Procss-ID + Thread-ID +  [logging-leve: E - error, W - warning, I - info, D - debug) + Message-Text
  ```

  The following is an example information message:

  ```
  May 23 12:53:51 2996 4014012160 [I] bfs_close_open_nodsp: File /00000004 opened in non-DSP mode
  ```

- DD Boost SDK precert log file
- DD File System logs

  DD File System logs are found on the system in the directory `/ddr/var/log/debug`. See the *DD OS Administration Guide* for more information.

BoostFS generates a local log file that contains its internal status, activities, warnings, and errors. You can specify the logging level in addition to the name and location of the log file by using the CLI or the BoostFS configuration file.

You might need to set a size limit on the log file to ensure that when the size of the log file reaches that limit, BoostFS will rotate log files.

You can configure the maximize size of the BoostFS log file in the configuration file. You can also configure the number of older log files you wish to keep.

When the log file size reaches the maximum specified size (in MB), the log file is renamed by appending ".1" to the log file name. If there is already an existing log file that ends in ".1," that file is renamed to replace ".1" with ".2." As each log file reaches the maximum size, log files with numbers (n) appended are renamed .n+1 up to the maximum log rotate number.

Known issues

Some common issues with BoostFS for Windows can be resolved quickly.

Installation fails

If installing BoostFS Windows fails, verify that:

- There is enough space on the drive on which you are installing BoostFS.
- The VeriSign Class 3 Public Primary Certification Authority - G5 is not blocked. This root certificate is used to sign the driver.

Mount fails

Troubleshooting mount issues on page 29 explains the causes and resolutions of several common errors that are encountered when mounting BoostFS.

Table 3. Troubleshooting mount issues

Error message	Cause	Resolution
`Mount failed with error code 183: Cannot create a file when that file already exists.`	This error occurs when a mount has the same PowerProtect or Data Domain hostname and storage-unit name as an existing BoostFS mount.	To map a drive to the same mount, use the `net use` command.
`Cannot mount mount-point: unexpected error, please see log for details.`	This error usually occurs when the DD Boost protocol is not enabled and configured on the PowerProtect or Data Domain system.	Review the BoostFS log files for more details. Use the `ddboost status` command in DD OS to confirm that DD Boost is enabled.
`Invalid mount point option and value pair [option=key from config file ] [value= value from config file]: Configuration initialization failed`	This message can appear when errors occur during the processing of the BoostFS configuration file.	Review the specific key and value in the BoostFS configuration file and make any necessary corrections.

Explorer performance degraded

If the Properties window for files or directories loads slowly, ACLs cannot be set from the Explorer interface, or both, verify that port 445 is not blocked from the client to the PowerProtect or Data Domain system. These issues occur because SMB messages over port 445 are used to determine the system security configuration.

To resolve both issues, unblock the SMB port. Alternatively, you can set ACLs using the Windows command prompt or PowerShell.

Access denied when using ACLs

To perform operations on a file or directory that is a child of a directory, the `traverse folder` permission is required on the parent directory, in addition to any other applicable permissions. This includes, but is not limited to, creating or deleting a child file or directory.

For example, to delete the file `M:\parent\child.txt`, both `traverse folder` and `delete subfolders and files` permissions are required on `M:\parent`, as well as `delete` permissions on `M:\parent\child.txt`.

To delete a directory, the `list folder` and `delete` permissions are required because Windows checks that a directory is empty before deleting it.

Kerberos

The following section describes Kerberos common errors and solutions:

`Insufficient access to or storage-unit storage-unit does not exist`

If this error is encountered while mounting BoostFS, use the `boostfs kerberos query` command to confirm that a valid Kerberos ticket exists for the storage-unit user. Use the `boostfs kerberos set` command to reconfigure the expired ticket if necessary.

NOTE: If the BoostFS debug log contains the error message `Server not found in Kerberos database`, confirm that the DNS entries are correct and you can perform a forward and reverse DNS lookup of the server hostname.

`Windows can't access this disc. The`

If this error is encountered while trying to access BoostFS mount point, confirm that a valid Kerberos ticket exists for the user accessing the BoostFS mount point.

disc might be corrupt.

A

Appendix

Topics:

References

The following documents, located at Online Support, provide additional and relevant information. Access to these documents depends on your login credentials. If you do not have access to a document, contact a sales representative.

- *Data Domain BoostFS Integration Guide: Application Validation and Best Practices*, available on https://community.emc.com
- *DD OS Administration Guide*