Document Storage Options for Installations of Content Platform Engine

Contents

Introduction

This document provides details on the different options for storing document content. In addition to the options described in this document, content can also be stored in an object store database. For more information on configuring storage for an object store, refer to the following topic in the online documentation: https://www.ibm.com/docs/en/filenet-p8-platform/5.5.11?topic=infrastructure-storing-content

This document is divided into the following sections:

- A synopsis of the supported storage types for each available storage method
- Storage limitations for containerized environments
- General file system information
- General fixed content device information
- Details on each of the supported storage types. The storage types are listed in alphabetic order
- Storage types that are deprecated

Section 1: Storage Methods

The following table lists in alphabetic order the types of storage that are supported with FileNet Content Engine and identifies the type of methods that can be used to define the storage in ACCE. Use the links in the Storage Type column to review detailed information about a specific storage type.

Storage types that are deprecated are not listed in the table. Links are provided to the detailed information about each storage type. Deprecated storage types are not listed in the table, instead these storage types are described in Section 4: Deprecated Storage Options at the end of this document.

Storage Method / Storage Type	Fixed content device	Advanced Storage	File System	Can be used with CPE Containers
Azure Blob Storage		✓		✓
AWS S3 Compatible Devices	✓	✓		✓
Ceph Object Storage	✓	✓		✓
CIFS and NFS-compatible storage devices		✓	✓	NFS-compatible storage is supported
Dell EMC Atmos Cloud Storage	✓			
Dell EMC Elastic Cloud Storage	✓	✓		✓
Dell EMC Isilon/PowerScale	✓			
Google Cloud Storage	✓	✓		S3 interface is supported
GPFS		✓	✓	Supported as NFS-compatible storage
Hitachi Cloud Scale	✓	✓		S3 interface is supported
Hitachi Content Platform	✓	✓		✓
IBM Cloud Object Storage	✓	✓		S3 interface is supported
IBM Spectrum Protect	✓			✓
NetApp ONTAP Snaplock	✓		✓	✓

Storage Method / Storage Type	Fixed content device	Advanced Storage	File System	Can be used with CPE Containers
NetApp Storage Grid	✓	✓		S3 interface is supported
RedHat OpenShift Data Foundation		✓		✓
Spectrum Scale		✓	✓	Supported as NFS-compatible storage

Section 2: Storage Choices for Content Platform Engine Containers

In general, the same storage choices are available for both traditional and containerized installations of Content Platform Engine. The differences are explained in the following table.

Storage Option	Limitations for Containerized Content Platform Engine
CIFS-compatible storage devices	Not supported
NFS-compatible storage devices	Limited to a single mount point
File System Encryption	SM4 encryption is supported
Dell EMC Atmos Cloud Storage	Not supported

Section 3: File System Information

This section provides general information on using file storage for document content. The file storage can be configured to be traditional file storage or advanced storage.

File Systems

Content Platform Engine requires:

- POSIX-compliant file systems on UNIX and Linux platforms
- NTFS-compatible file systems on Microsoft Windows platforms

IBM supports Content Platform Engine with any file system that meets the stated requirements, including Amazon Cloud Native Elastic File System. However, be aware that file systems with high latency can experience performance problems. If threads are blocked waiting for I/O to complete, severe resource contention and poor performance can result.

File systems are required to be in read/write mode; file systems in write once, read many (WORM) mode are not supported as file storage areas, staging areas, or cache areas.

CIFS and NFS-compatible storage devices

Content Platform Engine supports Magnetic Network Attached Storage (NAS) devices that enable access through the Network File System (NFS) or Common Internet File System (CIFS). However, NAS heads fronting Hierarchical Storage Management (HSM) systems are not supported.

File locking must be enabled. For NFS v3 this is usually provided by Network Lock Manager which is a separate service that must be enabled.

To ensure reliable operation and prevent possible corruption or loss of data, use

- NFS version 3 or NFS version 4 with at least an Uninterruptible Power Supply (UPS) backup device for mitigating power-off scenarios.
- Implement a highly available storage system.

Connections to remote file stores must use NFS for UNIX and CIFS for Windows.

Note: IBM requires implementing the -**noac** option when presenting storage to Content Platform Engine servers over an NFS mount. Using the default NFS mount options can result in data loss. Refer to the following technote for more information:

https://www.ibm.com/support/pages/filenet-content-manager-potential-data-loss-when-documents-are-written-nfs-mounted-disk-volume-and-disk-volume-full-or-near-full-capacity

Distributed File Systems

Content Platform Engine supports DFS for name resolution but does not support the DFS replication feature.

File System Encryption Technology

Content Platform Engine can be configured to encrypt content in a storage area. Two forms of encryption are supported:

- AES in Counter mode, a Federal Information Processing Standard (FIPS) 140-compliant algorithm, with a 128-bit key or a 256-bit key.
- SM4 encryption using a JCE provider with an SM4 implementation, such as Bouncy Castle.

  The bouncycastle.jar 1.73 and later are supported.

Refer to the following topic in the documentation for information on this capability:

https://www.ibm.com/docs/en/filenet-p8-platform/5.5.11?topic=stored-content-encryption

Some encryption technologies are designed to be, and are advertised as being, transparent to applications and communication channels to and from storage. IBM has not tested these claims. Although no specific integration effort may be required for the use of these technologies with P8 software, performance might still be affected.

IBM supports its software deployed in environments using these products unless otherwise noted. However, while troubleshooting issues, if IBM determines the issue is related to the

encryption product, IBM can require that the customer reproduce the problem in an environment without file system encryption.

File storage areas on encrypted NTFS devices are not supported.

Section 4: Fixed Content Devices

Fixed content devices are devices that are classified as Write Once Read Many (WORM) devices. Several of the supported storage options can be

- Configured as different types of Fixed Content Devices, as well as Advanced Storage and File System Devices.
- Configured to coordinate retention settings on the Content Platform Engine and those set on the storage.

  Content Platform Engine supports the following retention settings; however, not all storage types that can be configured as fixed content devices can be used with each of these retention options.

  - None
  - Indefinite
  - Fixed
  - Permanent

  The S3 compatible devices can be configured either as Advanced Storage Area Devices or as Fixed Content Devices. When configured as Fixed Content Devices in aligned mode, storage-level, fixed-based retention is supported.

  Refer to this topic for more information on setting retention: https://www.ibm.com/docs/en/filenet-p8-platform/5.5.11?topic=objects-retaining

- Configured to use device holds to prevent the content from being deleted from the storage side even if the configured retention period has expired. For more information on device holds, refer to the following topic: https://www.ibm.com/docs/en/filenet-p8-platform/5.5.11?topic=areas-v552-later-using-device-holds

  Currently the following storage types support device holds:

  - Storage devices configured as S3 Fixed Content Devices
  - Elastic Cloud Storage
  - Hitachi Content Platform
  - IBM Cloud Object Storage

Refer to the detailed information on each storage type in this document, as well as to the information in this topic: https://www.ibm.com/docs/en/filenet-p8-platform/5.5.11?topic=infrastructure-storing-content to determine the configuration that best supports your use cases.

Section 5: Supported Storage Types

Azure Blob Storage

Microsoft Azure Blob Storage is supported as an advanced storage area. For information on configuring this type of storage, refer to the following technote: https://www.ibm.com/support/pages/node/6347172.

Amazon S3 Compatible Devices

Content Platform Engine supports the Amazon S3 connection interface. Storage devices that fully implement the Amazon S3 storage interface can usually be supported.

Refer to the following tech note for additional information and requirements: https://www.ibm.com/support/pages/node/744379.

The following table lists the specific devices that have been qualified and identifies which ones can be used as S3 Advanced Storage Devices and as S3 Fixed Content Devices.

Storage Method / Storage Type	S3 Advanced Storage Device	S3 Fixed Storage Device	Comments
Amazon Storage	X	X	
AWS S3 Glacier Instant Retrieval Storage	X		Requires Glacier Instant Retrieval storage class. There is no support for configurations that use the Glacier Flexible Retrieval or Glacier Deep Archive classes.
Ceph Object Storage	X	X	
Dell EMC Elastic Cloud Storage (ECS)	X	X	Minimum level is ECS 3.6.2
Google Cloud Storage	X	X	Refer to the following technote for information on additional restrictions: https://www.ibm.com/support/pages/using-google-cloud-storage-s3-advanced-storage-device-content-platform-engine
Hitachi Cloud Scale	X	X	
Hitachi Content Platform Platform (HCP)	X	X	Version 9.4 is the minimum supported level
IBM Cloud Object Storage (ICOS)	X	X	
Multicloud Object Storage	X	X	
Nutanix S3	X	X	
Red Hat OpenShift Data Foundation (ODF) object storage	X	X	Includes Ceph Object Storage and Multicloud Object Storage

Ceph Object Storage

If Ceph Object storage is configured as an S3 Fixed Content Device, to use the aligned retention mode feature of the Fixed Content Device, the Ceph Object Storage bucket must be object-lock enabled.

Dell EMC ATMOS Cloud Storage

ATMOS Cloud Storage can be used as a fixed content device.

Support is provided for version 2.1.6.1.

ATMOS compliant subtenants are not supported.

Dell EMC Elastic Cloud Storage (ECS)

Any version of ECS that provides an S3 interface can be used as an S3 advanced storage area. To configure ECS as an S3 advanced storage area, refer to the following topic in the documentation:

https://www.ibm.com/docs/en/filenet-p8-platform/5.5.11?topic=devices-creating-s3-storage-device

Starting with the 3.6.2 release, ECS can be used as an S3 Fixed Content Device.

CPE supports ECS 3.6.2 and later (for instance 3.8.x) as an S3 fixed content device. When using ECS as an S3 fixed content device, event-based retention is not supported. S3 fixed content devices can use only fixed retention. Device holds are supported in this configuration.

ECS can also be configured as a Centera fixed content device using the CAS SDK. Refer to the following section for information on the CAS SDK: Dell EMC Centera SDK Support.

Namespace Retention Policy is not supported and should not be set on the namespace. Similarly, the retention class on Centera storage is not supported.

Important: The CAS SDK is not supported on zLinux. As the CAS SDK must be installed on the Content Platform Engine server, ECS cannot be supported as a Centera Fixed Content Device when Content Platform Engine is deployed on zLinux.

The minimum supported level of ECS is 3.0. Be aware of the following caveats when using ECS as a fixed content device using the CAS SDK:

- EMC Elastic Cloud Storage 3.0.x

  Both fixed and event-based retention are supported with this version of ECS.

  Elastic Cloud Storage 3.0 adds support for the Centera event-based retention features.

  Due to an issue with zero length content, the recommended minimum level of this version of ECS is 3.0 HF2.

- EMC Elastic Cloud Storage 3.1 and above

  Both fixed and event-based retention are supported with these versions of ECS.

Dell EMC Centera SDK Support

Content Platform Engine can be configured to store content in Dell EMC Centera Basic, Governance, and Compliance Edition Plus storage devices. This capability is supported with the Centera SDK provided on the Content Platform Engine media and includes all higher versions of CentraStar that are compatible with this version of the SDK.

Dell EMC Elastic Cloud Storage (ECS) can also be configured to use the Centera SDK.

Refer to the Dell EMC documentation for a CentraStar and SDK Release and Interoperability Matrix.

Starting in Content Platform Engine 5.5.9, the CAS SDK is included in the Content Platform Engine container images for Linux.

Support is limited to the functionality described in the P8 documentation.

New CentraStar features are not automatically supported.

Installing any version of the Centera SDK on the Content Platform Engine server, in whole or in part over the version installed with the Content Platform Engine, is not supported.

CAS SDK

The Centera 3.3 SDK provided with Content Platform Engine. Refer to the following topic of instructions on installing the SDK on a traditional Content Platform Engine server: https://www.ibm.com/docs/en/filenet-p8-platform/5.5.11?topic=iuecslf-installing-emc-centera-sdk-library-files. The Content Platform Engine container includes the CAS SDK. The following table provides the specific Centera SDK version included in the CPE installer. Refer to the Dell EMC documentation for additional information.

Important: The Centera SDK is not supported on zLinux.

Operating System	Centera SDK Version
AIX	3.3.721
Linux	3.3.719
Windows	3.3.718

Dell EMC Isilon/PowerScale

Note that as of version 9, Dell EMC Isilon has been renamed PowerScale.

Support is provided for One FS

- Version 7.2.x and 8.x in SmartLock Enterprise Mode and Compliance Mode

- Version 9.1 and 9.2 in SmartLock Enterprise Mode and Compliance Mode provided that the vendor documents the new release as backward compatible. Version 9.3 is not supported. To connect to PowerScale 9.1 or 9.2 use the same interface as is being used with your current Isilon/PowerScale release. If an issue occurs that requires an architectural change in Content Platform Engine, the required update will be provided in a future Content Platform Engine release.
- Newer versions (9.3 and above) are not supported

There are some limitations when using an Isilon OneFS cluster in Compliance Mode

- When creating the Isilon fixed content device, use the compliance "root" user (compadmin) instead of an ordinary user.
- Use the out-of-the-box "ifs" access point instead of creating new RAN access points

See the following topic in the documentation for additional information on configuring Dell EMC Isilon as a fixed content device:

https://www.ibm.com/docs/en/filenet-p8-platform/5.5.11?topic=device-configuring-isilon-smartlock

General Parallel File System (GPFS) and Spectrum Scale Support

GPFS 4.1 or later, and Spectrum Scale 4.1.1 or later, are supported on Linux and AIX for file storage areas, fixed content staging areas, and content cache areas.

File stores hosted on GPFS or Spectrum Scale file systems can be accessed directly if the Content Platform Engine server is a member of the GPFS or Spectrum Scale cluster or by mounting the devices as remote file systems using NFS version 4.

When Content Platform Engine servers are accessing GPFS or Spectrum Scale file systems using the Network File System (NFS) protocol, NFS version 4 must be used. NFS Version 4 is required because the Content Platform Engine makes extensive use of file locking for content cache areas. The default file locking semantics on GPFS and Spectrum Scale are not compatible with NFS version 3 or earlier.

Important: IBM requires implementing the **-noac** option when presenting storage to Content Platform Engine servers over an NFS mount. Using the default NFS mount options can result in data loss. Refer to the following tech note for more information:

https://www.ibm.com/support/pages/filenet-content-manager-potential-data-loss-when-documents-are-written-nfs-mounted-disk-volume-and-disk-volume-full-or-near-full-capacity

For additional information on configuring Spectrum Scale with Content Platform Engine, refer to the following Redbooks publication:

http://www.redbooks.ibm.com/abstracts/redp5239.html?Open

Google Cloud Storage

Google Cloud Storage can be configured as an S3 advanced storage area or as a fixed-content device. There are constraints with both configurations. Refer to the following technotes for details:

- Using Google Cloud Storage as an advanced storage area: https://www.ibm.com/support/pages/using-google-cloud-storage-s3-advanced-storage-device-content-platform-engine
- Using Google Cloud Storage as a fixed content device: https://www.ibm.com/support/pages/node/6497387

Hitachi Cloud Scale

Using the generic S3 connector, Content Platform Engine supports Hitachi Cloud Scale as both an advanced storage area and as a fixed content device. When Hitachi Cloud Scale is used as a fixed content device, only fixed content retention is supported; event-based retention and permanent retention are not supported.

Hitachi Content Platform

Content Platform Engine supports Hitachi Content Platform 8.x, and 9.x as a fixed content device.

Hitachi Content Platform 9.4 and later can also be used as an S3 Advanced Storage Device using the S3 interface. Hitachi Content Platform 9.4 is not supported as an S3 Fixed Content Device. However, Hitachi Cloud Scale can be used as an S3 Fixed Content Device.

Using Hitachi Content Platform as a Fixed Content Device

Be aware of the following when using HCP as a fixed content device:

- Authenticated Hitachi Content Platform namespaces in both compliance and enterprise mode are supported.
- The default namespace is not supported.
- The Content Platform Engine communicates with Hitachi Content Platform using the HTTP REST interface, and both HTTP and HTTPS (SSL) transports are supported.
- No separate client software is required to use Hitachi Content Platform as a Content Platform Engine fixed content device.
- The Hitachi Content Platform is not FIPS certified.
- Device holds are supported.

Using Hitachi Content Platform as an S3 Advanced Storage Area

If you are using a version-enabled HCP bucket, and want to delete a specific version by setting the Content Platform Engine configuration parameter *Advanced.S3.DeleteSpecificVersion* to true, you must enable the following versioning options on the HCP bucket (namespace):

- Allow overwrite of objects via Hitachi API for AWS S3 if version is disabled
- Enable delete markers

Important: The Hitachi Content Platform cannot be used as a CIFS or NFS mounted file system as the root directory for a file storage area or the staging directory of a fixed storage area as Hitachi Content Platform is a WORM device that does not allow the file operations needed by the Content Platform Engine.

IBM Cloud Object Storage (ICOS)

ICOS can be configured as

- An advanced storage device
- An ICOS fixed content device
- An S3 fixed content device

When ICOS is configured as an advanced storage area, you can use Content Platform Engine event and fixed-based retention with documents that are stored on the device.

However, if you need to set retention on the storage device, then configure ICOS as a fixed content device. Content Platform Engine and storage-level retention can be coordinated by configuring the fixed content device in aligned mode.

Both ICOS fixed-based and event-based retention are supported when ICOS is configured as an ICOS fixed content device, but when configured as an S3 fixed content device, event-based retention is not supported.

To use the ICOS retention management, ensure the ICOS vault is protection enabled.

If you are configuring ICOS storage for the first time and there is a potential that in the future storage retention management might be required,

- Define an ICOS fixed content device in unaligned mode
- Ensure the vault is protection enabled
- Set the minimum retention to zero

Device holds are supported.

IBM Spectrum Protect

IBM Spectrum Protect can be configured as a fixed content device. (IBM Spectrum Protect was previously named IBM Tivoli Storage Manager. See the following technote for more details: https://www.ibm.com/support/pages/node/534193.)

Content Platform Engine can be configured to store content in an IBM Spectrum Protect 8.1.x server and in IBM Tivoli Storage Manager Server 7.1.x.

Minimum supported IBM Spectrum Protect Client is 7.1.6.3.

Refer to the following technote for information on supported IBM Spectrum Protect client and server combinations: https://www.ibm.com/support/pages/node/660949.

The IBM Spectrum Protect Client must be installed on the Content Platform Engine server.

Be aware of the following when using IBM Spectrum Protect:

- Storage behind the Information Archive or any other IBM Spectrum Protect server is supported with the following caveats:
  - Tape storage support is limited to near-line media that can be readily and transparently mounted for content retrieval.
  - Offline tape is not supported.
  - No form of end-user notification of an offline tape coming online is supported.
- Optical, Centera and SnapLock media are not supported as storage behind IBM Spectrum Protect, or Information Archive.

For Information Archive:

- Only the IBM Spectrum Protect for Data Retention interface that uses the Tivoli Storage Manager API is supported.
- File system interfaces such as NFS and CIFS are not supported.

Virtualization Restrictions

Refer to the following technical notice for information on the IBM Spectrum Protect and IBM Tivoli Storage Manager virtualization restrictions.

https://www.ibm.com/support/pages/node/83755

NetApp ONTAP SnapLock

Content Platform Engine can be configured to store content in Network Appliances or IBM N-series SnapLock-enabled storage devices using a CIFS or NFS mount.

Connections to remote file stores must use NFS for UNIX and CIFS for Windows.

SnapLock Enterprise and Compliance Editions are supported.

Important: IBM requires implementing the **-noac** option when presenting storage to Content Platform Engine servers over an NFS mount. Using the default NFS mount options can result in

data loss. Refer to the following technote for more information:

https://www.ibm.com/support/pages/filenet-content-manager-potential-data-loss-when-documents-are-written-nfs-mounted-disk-volume-and-disk-volume-full-or-near-full-capacity

The following can be configured as SnapLock fixed content devices:

- NetApp Data ONTAP 8.1.x (7-Mode)
- NetApp Data ONTAP 8.2.x (7-Mode) -- minimum level 8.2.1
- NetApp ONTAP 9.x SnapLock in Cluster mode

Other NetApp Data ONTAP versions configured in cluster mode cannot be used as fixed content devices as they do not provide SnapLock support.

Note: The Content Platform Engine SnapLock implementation does not support SnapLock indefinite retention, and permanent retention is set to the maximum retention allowed on individual files by SnapLock (01/19/2071). Permanent and indefinite retention are handled by Snaplock using the default volume retention setting and cannot be set using a "file last access" time.

NetApp StorageGRID

Using the generic S3 connector, Content Platform Engine supports NetApp StorageGRID as both an advanced storage area and as a fixed content device. When NetApp StorageGRID is used as a fixed content device

- The minimum supported level is 11.5
- Only fixed content retention is supported; event-based retention is not supported.

Section 6: Deprecated Storage Options

Hadoop File System

This capability is deprecated.

The Hadoop File System is supported as an advanced storage area.

Requires Apache Knox Gateway 0.7.0. The Knox Gateway is installed on the Hadoop cluster and serves as a central point to expose all the Restful API services for Hadoop.

OpenStack Advanced Storage Devices

This capability is deprecated.

For information on creating an OpenStack Cloud Storage Device, see the FileNet P8 Platform documentation:

https://www.ibm.com/docs/en/filenet-p8-platform/5.5.11?topic=areas-advanced-storage-devices

Support is provided for OpenStack Storage API v1, using OpenStack Storage API v1 authentication or OpenStack Identity API v2 authentication.

Spectrum Scale on GPFS extension device v4.1.1.1 support

Spectrum Scale can be used as a storage device, using the OpenStack Identity API v2.0.

When configuring a Spectrum Scale OpenStack advanced storage device, the device URL must be supplied in the Identity API v2.0 format.