Contents

NFS-compatible storage devices

Content Platform Engine supports Magnetic Network Attached Storage (NAS) devices that enable access through the Network File System (NFS). 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 which much 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.

Note: IBM recommends implementing the **-noac** option when presenting storage to Content Platform Engine servers over an NFS mount. Using the default NFS mount options could result in data loss in certain circumstances. Please 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

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 using 128-bit or 256-bit encryption. Refer to the following topic in the Knowledge Center for more information on this capability:

http://www.ibm.com/support/knowledgecenter/en/SSNW2F_5.5.0/com.ibm.p8.ce.admin.tasks.doc/contentstores/cs_content_encryption.htm

Some encryption technologies are designed to be, and 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, if in the course of troubleshooting its software, IBM determines an 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.

Spectrum Scale

Spectrum Scale 5.1.1 or later are supported for advanced file storage areas, file storage areas, fixed content staging areas, and content cache areas.

If using a traditional Spectrum Scale cluster, configure the storage using CNSA/CSI. If the Spectrum Scale cluster is deployed in OpenShift, configure the storage using CSI.

Initial storage requirements can be generated using the Persistent Volume Claim (PVC) for the Content Platform Engine container. If additional storage directories are required after deployment, create the empty directories using mkdir on the existing PVC.

File Systems

IBM supports Content Platform Engine using with any file system, including Amazon Cloud Native Elastic File System. However, customers should 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.

S3 Advanced Storage Areas

Content Platform Engine supports the Amazon S3 connection interface to many storage devices including Amazon Storage, Dell Elastic Cloud Storage (ECS), and IBM Cloud Object Storage (ICOS). Use the Generic S3 Advanced Storage Device option in ACCE to use a storage device

via an S3 connection. 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/docview.wss?uid=ibm10744379.

Google Cloud Storage is also supported as an advanced storage area using the Generic S3 Advanced Storage Device connector; however, there are some additional constraints. Refer to the following tech note for details: https://www.ibm.com/support/pages/using-google-cloud-storage-s3-advanced-storage-device-content-platform-engine

Dell EMC Elastic Cloud Storage (ECS)

Content Platform Engine container can be configured to use ECS as a fixed content device and as an S3 Advanced Storage Area. When ECS is used as a fixed content device, the CAS interface is used.

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 Knowledge Center:
https://www.ibm.com/support/knowledgecenter/en/SSNW2F_5.5.0/com.ibm.p8.ce.admin.tasks.doc/p8pcc470.htm

CPE supports ECS 3.2.x, ECS 3.3.x, and ECS 3.4.x as Centera Fixed Content Devices using the CAS interface. Both fixed and event-based retention are supported with these versions of ECS.

The configuration for Elastic Cloud Storage as a Fixed Content Device is identical to the configuration for a Centera Fixed Content Device.

IBM Cloud Object Storage (ICOS) with Retention Management

When ICOS is configured as an advanced storage area, you can use CPE 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. CPE 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 a fixed content device in aligned mode.

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

If content is stored on ICOS that is configured as an advanced storage area and there is a need to apply storage-level retention to the content, define an ICOS fixed content device and then use the CPE sweep framework to move the content from the ICOS advanced storage area to the ICOS fixed content device.

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, use an ICOS fixed device in unaligned mode and ensure the vault is protection enabled and that the minimum retention is set to zero.

Hitachi Content Platform

Content Platform Engine supports Hitachi Content Platform 6.x, 7.x, 8.x, and 9.x 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) 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 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 file operations needed by the Content Platform Engine.

For performance reasons, Hitachi does not recommend using the S3 interface for Hitachi Content Platform.

The Hitachi Content Platform is not FIPS certified.

Device Holds are supported.

Amazon S3 Retention Management

The Amazon S3 connector can be configured either as an Advanced Storage Area Device or as a Fixed Content Device. When configured as a Fixed Content Device in aligned mode, storage level fixed-based retention is supported.

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.

SnapLock Enterprise and Compliance Editions are supported.

Note: IBM recommends implementing the **-noac** option when presenting storage to Content Platform Engine servers over an NFS mount. Using the default NFS mount options could result in data loss in certain circumstances. Please 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

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.