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 documentation for more information on this capability:

https://www.ibm.com/docs/en/filenet-p8-platform/5.5.x?topic=stored-content-encryption

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 Red Hat OpenShift Data Foundation (ODF) object storage, Nutanix S3, Amazon Storage, Dell Elastic Cloud Storage (ECS), Hitachi Cloud Scale, and IBM Cloud Object Storage (ICOS). Use the Generic S3 Advanced Storage Device option in ACCE to configure an S3 storage device 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/pages/node/744379.

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.

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

Red Hat® OpenShift® Data Foundation including Ceph Object Storage and Multicloud Object Storage features is supported as an advanced storage area.

The Ceph Object storage can also be 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.

The Multicloud Object Storage can be configured only as an S3 Advanced Storage Device.

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.

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.x?topic=devices-creating-s3-storage-device

CPE supports ECS 3.2 and above as Centera Fixed Content Devices using the CAS SDK. Both fixed and event-based retention are supported with these versions of ECS. In this configuration for Elastic Cloud Storage as a Fixed Content Device is identical to the configuration for a Centera Fixed Content Device.

The CAS SDK is installed as part of the CPE container. And since the CAS SDK is only supported on the Linux x86 operating system. If the container is running on any other version of Linux, use ECS as an S3 fixed content device or as an S3 advanced storage area.

CPE supports ECS 3.6.2 and later (for instance 3.8.x) as an S3 fixed content device. In this configuration, only fixed retention is supported. Device holds are supported in this configuration.

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.

Device holds are supported.

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; variable retention is not supported.

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.

The Hitachi Content Platform is not FIPS certified.

Device holds are supported.

Dell EMC Isilon/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 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.

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

The Dell EMC Isilon SmartConnect feature is available with version 8.0 and higher. To use this feature, configure authorization headers between Isilon and CPE.

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

- 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.x?topic=device-configuring-isilon-smartlock

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.

Device holds are supported.

IBM Spectrum Protect

IBM Spectrum Protect was previously named IBM Tivoli Storage Manager. See the following tech note for more details: https://www.ibm.com/support/pages/node/534193.

The IBM Spectrum Protect client is embedded in the Content Platform Engine container.

In the OpenShift container environment, before creating a Spectrum Protect (TSM) Fixed Content Device in ACCE, you must

- Import a Spectrum Protect Server certificate.
- Create a configuration file share folder.
- Create a fixed content storage area.

For detailed instructions, refer to the Cloud Pak for Automation documentation.

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

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:
    1. Tape storage support is limited to near-line media that can be readily and transparently mounted for content retrieval.
    2. Offline tape is not supported.
    3. 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

Portworx

Content Platform Engine Container supports Portworx 2.6.4 with Openshift 4.6 and up as an advanced storage area.

Portworx is a software-defined container storage, built from the ground up for Kubernetes. It enables high availability with asynchronous replication on multizone availability clusters.

To achieve high resiliency, set up replication across three zones, with shared storage access across multiple pods and worker nodes.

The configuration must support dynamic storage provisioning with ReadWriteMany (RWM) access on the persistent volumes. Storage classes can be customized.

For high availability/disaster recovery (HADR), configure at least 3 worker nodes in the Portworx cluster so that Portworx can replicate your data across nodes. For even higher availability, use a multizone cluster and replicate your volumes on SDS worker nodes across 3 zones.

For more information, refer to
https://docs.portworx.com/portworx-install-with-kubernetes/cloud/ibm/

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.

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; variable retention is not supported.

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 either configuration. Refer to the following tech notes 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