



IBM FileNet Content Manager 5.7'nin Red Hat OpenShift Üzerinde Production Kurulumu

Operator tabanlı kurulumdan kalıcı depolamaya uçtan uca teknik yaklaşım

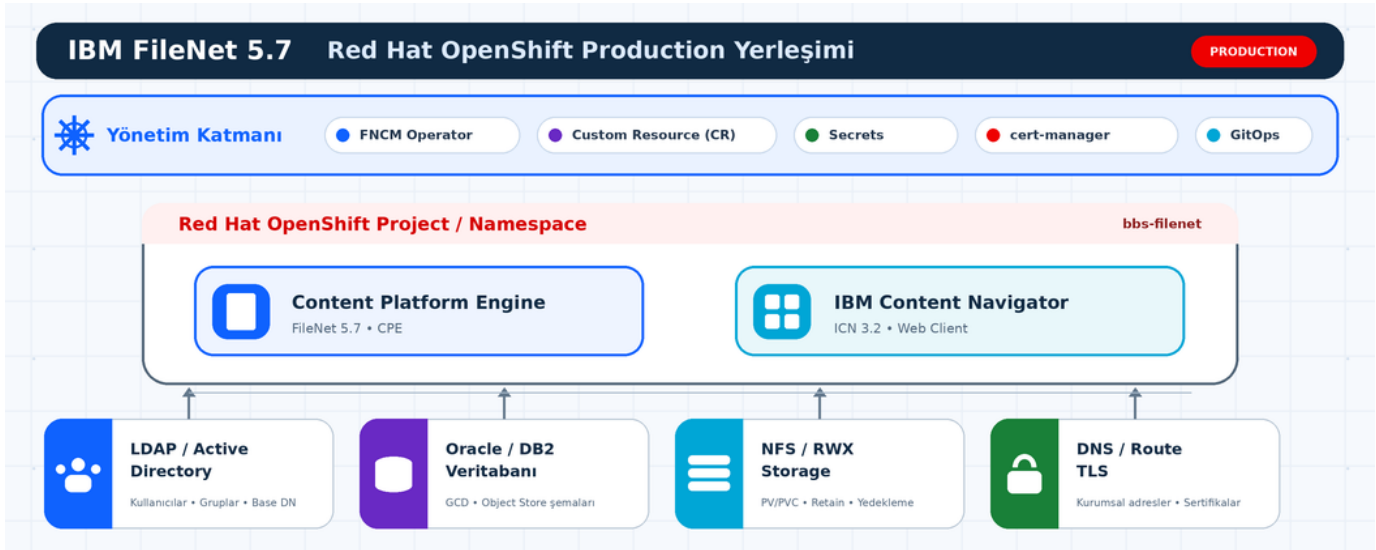
Erkan Sezer | IBM İş Uygulamaları Müdür Yardımcısı, Bilgi Birikim Sistemleri (BBS)

Özet

IBM FileNet Content Manager'ın container mimarisine taşınması yalnızca pod'ların çalıştırılması değildir; kimlik, veri tabanı, kalıcı depolama, sertifika, route ve yaşam döngüsü yönetiminin tek bir production tasarımında birleştirilmesidir. Bu makale, IBM FileNet Content Manager 5.7 ve IBM Content Navigator 3.2'nin Red Hat OpenShift üzerinde konumlandırılmasını; Operator, Custom Resource (CR), LDAP, Oracle/DB2, IBM Entitlement Key ve statik NFS PV/PVC bileşenleri üzerinden adım adım ele alır.

Temel ilke CR dosyası hedef durumu tanımlar; FNCM Operator bu hedefi sürekli uzlaştırır. Bu nedenle CR, secret ve storage tanımlarının sürüm kontrollü ve ortam bazlı yönetilmesi production güvenilirliğinin merkezindedir.

Hedef Mimari



Kurulum Başlamadan Önce

OpenShift Desteklenen OCP sürümü, worker kapasitesi, DNS/route ve registry erişimi	Kimlik LDAP/AD bind hesabı, kullanıcı-grup Base DN'leri ve yönetici grupları	Veri tabanı En az GCD ve Object Store şemaları; JDBC erişimi ve yedekleme politikası
Depolama RWX destekli storage class veya statik PV/PVC; Retain ve kapasite planı	Güvenlik IBM Entitlement Key, secrets, TLS sertifikaları ve en az ayrıcalık	Operasyon İzleme, log toplama, RPO/RTO, geri dönüş ve bakım penceresi

1. OpenShift Project, Operator ve Custom Resource

1	Project oluşturma — Linux bastion üzerinden “oc new-project bbs-filenet” komutuyla yaratılmış bir namespace oluşturulur. ResourceQuota, LimitRange, NetworkPolicy ve RBAC kararları uygulama kurulmadan önce netleştirilmelidir.
2	Operator kurulumu — OpenShift Console’daki IBM FNCM kataloğundan FileNet Content Manager Operator kurulur; ayrıca sertifika yaşam döngüsü için cert-manager Operator’ın durumu `Succeeded` olmalıdır. Operator logları kurulum ve uzlaştırma hatalarının ilk inceleme noktasıdır.

Temel doğrulama komutları

```
oc project bbs-filenet
oc get csv -n bbs-filenet
oc logs -f deployment/ibm-fncm-operator -c operator
```

3	CR kapsamını belirleme — İlk aşamada yalnız CPE kurulacaksa “cpe: true”; CMIS, CSS, External Share, Task Manager ve GraphQL gibi kullanılmayan bileşenler “false” tutulur. IBM Content Navigator daha sonra aynı CR ve aynı Operator üzerinden “ban: true” ile eklenebilir.
---	--

Bileşen seçimi – sadeleştirilmiş örnek

```
content_optional_components:
  cmis: false
  css: false
  es: false
  tm: false
  cpe: true
  graphql: false
  ban: false
```

2. LDAP, Veri Tabanı ve Secret Tasarımı

FileNet domain’i ve Object Store’lar, kimlik dizini ve ilişkisel veri tabanı ile sıkı biçimde bağlıdır. CR uygulanmadan önce bağlantı testleri, DNS çözümlemesi, port erişimi, sertifika zinciri ve servis hesaplarının yetkileri “bastion” ve “pod” ağından doğrulanmalıdır.

LDAP / AD Bind hesabı; user/group Base DN; domain admin ve object store admin için ayrı gruplar.	Oracle / DB2 GCD için bir şema, her Object Store için ayrı şema; JDBC URL, servis adı ve havuz ayarları.	Secrets “ibm-fncm-secret” içinde DB, uygulama ve keystore kimlik bilgileri; CR içinde parola tutulmaz.
--	--	--

IBM belgeleri, FileNet P8 domain yöneticileri ile Object Store yöneticileri için farklı grupların kullanılmasını önerir. Böylece ekip üyeliği LDAP üzerinden yönetilebilir ve tek kullanıcı hesabına bağımlılık azaltılır. FIPS etkinse keystore ve bazı veri tabanı parolaları için uzunluk koşulları ayrıca kontrol edilmelidir.

CR içindeki kritik referanslar

```
ecm_configuration:
  fncm_secret_name: ibm-fncm-secret
  cpe:
    hostname: filenet.example.com
    replica_count: <capacity-and-ha-plan>

shared_configuration:
  image_pull_secrets:
    - ibm-entitlement-key
```

Production Notu: Kaynak saha örneğinde “replica_count: 1” kullanılmıştır. Production ortamında replica sayısı, lisanslama, destek matrisi, kapasite testi, pod anti-affinity ve bakım/arıza senaryolarıyla birlikte belirlenmelidir; örnek değer doğrudan kopyalanmamalıdır.

3. İlk Dağıtım ve Gözlem

“initialize_configuration” bölümü FileNet domain ve Object Store nesnelerinin ilk oluşturulmasında kritiktir. İlk kurulumla genişletme/güncelleme senaryoları ayrılmalı, aynı altyapı yanlılıkla yeniden initialize edilmemelidir. CR uygulandıktan sonra Operator durumu, pod event’leri, deployment’lar, service ve route’lar birlikte izlenir.

Dağıtım ve çalışma durumu

```
oc apply -f ibm_fnm_article.yaml
oc get pods,deployments,svc,routes -n bbs-filenet
oc get events -n bbs-filenet --sort-by=.lastTimestamp
```

4. IBM Content Navigator 3.2’nin Aynı Mimariye Eklenmesi

IBM Content Navigator (ICN), FileNet kullanıcılarının belge, klasör, arama ve iş akışı yeteneklerine eriştiği web istemcisidir. Kaynak uygulamada ICN, “bbs-filenet” projesinde mevcut FNCM Operator ve mevcut CR genişletilerek devreye alınmıştır; ayrı bir Navigator Operator kurulmamıştır.

ICN ekleme – sadeleştirilmiş CR farkı

```
content_optional_components:
  cpe: true
  ban: true

navigator_configuration:
  ban_secret_name: ibm-ban-secret
  hostname: navigator.example.com
  replica_count: <capacity-and-ha-plan>

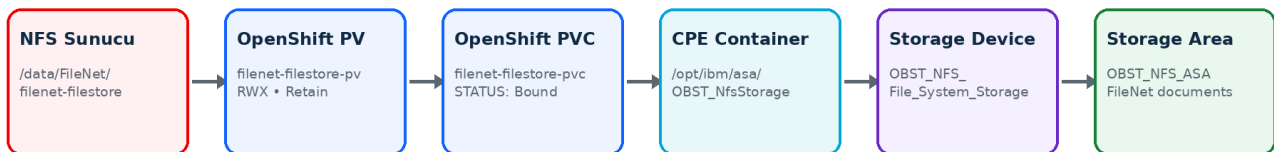
shared_configuration:
  sc_content_initialization: false
```

Neden “sc_content_initialization: false”? CPE daha önce kurulmuş ve Content Services altyapısı initialize edilmiştir. ICN eklenirken aynı altyapının yeniden initialize edilmesi istenmez. İlk kurulumda kullanılan değer ile sonraki genişletme adımı birbirinden ayrılmalıdır.

5. Statik NFS PV/PVC ve Advanced Storage Area

Production içerik depolamasında kalıcılık, uygulama pod’undan ayrıştırılmalıdır. IBM dokümanları statik veya dinamik provisioning’e izin verir; statik modelde PV ve PVC önceden oluşturulur, CR içinde mevcut claim adı referans edilir. Veri taşıyan FileNet volume’lerinde “ReadWriteMany” erişim modu ve “Retain” reclaim policy kritik iki kontroldür.

Belgenin Uçtan Uca Kalıcı Depolama Akışı



PV
apiVersion: v1
kind: PersistentVolume
metadata:
 name: filenet-filestore-pv
spec:
 capacity: {storage: 100Gi}
 accessModes: [ReadWriteMany]
 persistentVolumeReclaimPolicy: Retain
 storageClassName: managed-nfs-storage
 nfs:
 server: <nfs-server>
 path: /data/FileNet/filenet-filestore

PVC
apiVersion: v1
kind: PersistentVolumeClaim
metadata:
 name: filenet-filestore-pvc
 namespace: bbs-filenet
spec:
 accessModes: [ReadWriteMany]
 resources:
 requests: {storage: 100Gi}
 volumeName: filenet-filestore-pv
 storageClassName: managed-nfs-storage
 volumeMode: Filesystem

PVC’nin “STATUS” değeri “Bound” olmadan CR uygulanmamalıdır. CPE file store için claim, CR’de “datavolume.existing_pvc_for_cpe_filestore” altında tanımlanır. IBM’in volume tablosuna göre FileNet file-system tabanlı Advanced Storage Device’in container içindeki mount path’i “/opt/ibm/asa”dır.

Mevcut PVC'nin CPE'ye bağlanması

```
ecm_configuration:
  cpe:
    datavolume:
      existing_pvc_for_cpe_filestore:
        name: filenet-filestore-pvc
        size: 100Gi
```

ACCE Üzerinde Son Eşleme

- Administration Console for Content Platform Engine (ACCE) → Advanced Storage Areas → New Advanced Storage Area.
- Örnek alan adı: “OBST_NFS_ASA”; cihaz türü: File System Device; örnek cihaz adı: “OBST_NFS_File_System_Storage”.
- NFS üzerindeki “/data/FileNet/filenet-filestore/OBST_NfsStorage” klasörünün container karşılığı “/opt/ibm/asa/OBST_NfsStorage” olarak girilir.
- Test klasörüne belge eklenir; ACCE sayaçları ve NFS dizinindeki fiziksel dosya oluşumu birlikte doğrulanır.

6. Production İçin Kritik Kontroller

Alan	Kontrol	Kabul ölçütü
Kapasite / HA	Replica, CPU/RAM requests-limits, anti-affinity, PDB ve worker dağılımı	Bakım veya tek node kaybında servis hedefi korunur
Veri tabanı	GCD/OS şemaları, bağlantı havuzu, HA, bakım ve tutarlı yedek	Bağlantı testleri ve geri dönüş provası tamam
Storage	RWX, Retain, NFS/CSI performansı, quota, inode ve büyüme	PVC Bound; okuma-yazma ve geri yükleme testi başarılı
Kimlik	LDAP erişimi, Base DN, admin grupları, servis hesabı rotasyonu	Yönetici ve son kullanıcı oturumları doğrulanır
Güvenlik	TLS, route, secret yönetimi, RBAC, NetworkPolicy, registry erişimi	Açık metin parola yok; sertifika zinciri geçerli
Operasyon	Log/metric/alert, runbook, RPO/RTO, DR ve upgrade planı	İzleme ve geri dönüş senaryosu işletildi

7. Devreye Alma ve Doğrulama Akışı

1	Adım — CR ve secret manifestlerini Git üzerinden gözden geçirin; ortam değerlerini şablondan ayırın ve secret'ları repoya koymayın.
2	Adım — Operator/CSV, cert-manager, StorageClass, PV/PVC, DNS, LDAP ve DB bağlantılarını bağımsız olarak doğrulayın.
3	Adım — CR'yi uygulayın; Operator logları, event'ler, pod readiness, service ve route'ları izleyin. Hata durumunda semptomu değil ilk kök olayı bulun.
4	Adım — ACCE ping/erişim, FileNet domain ve Object Store; ardından ICN masaüstü, repository bağlantısı, arama, belge yükleme–indirme ve yetki testlerini çalıştırın.
5	Adım — Advanced Storage Area'ya test belgesi yazın; ACCE sayacı, container mount'u ve NFS fiziksel yolu arasında uçtan uca tutarlılık kontrolü yapın.
6	Adım — Performans tabanı alın, yedek/geri yükleme ve node bakım senaryosu uygulayın; yalnız teknik ve iş kabul kriterleri tamamlandığında production trafiğini açın.

Sonuç

IBM FileNet Content Manager 5.7'nin OpenShift üzerinde başarılı biçimde çalışması; Operator kurulumundan çok, bağımlılıkların disiplinli tasarlanmasına dayanır. Doğru ayrılmış LDAP grupları, bağımsız GCD/Object Store şemaları, güvenli secret yönetimi, production gereksinimine göre boyutlandırılmış replikalar ve RWX–Retain ilkelerine uygun kalıcı storage birlikte ele alındığında platform; ölçeklenebilir, izlenebilir ve yönetilebilir bir kurumsal içerik hizmetine dönüşür. Kaynak seride gösterilen CR yaklaşımı ile statik NFS zinciri, bu dönüşüm için uygulanabilir bir saha modeli sunmaktadır.