Building a Sovereign Cloud with Red Hat OpenShift (DO505) Eğitimi

Süre: **5 Gün**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

Dijital Egemenlik Gereksinimlerine Uygun Bulut Platformları Tasarlama ve İşletme

Building a Sovereign Cloud with Red Hat OpenShift (DO505) eğitimi, dijital egemenlik gereksinimlerini karşılayan, çok kiracılı, güvenli ve mevzuata duyarlı cloud platformlarının Red Hat OpenShift kullanılarak nasıl tasarlanacağını, kurulacağını ve işletileceğini öğretir.

Eğitim; enterprise architect'ler, IT security profesyonelleri ve operasyon ekipleri için hazırlanmıştır ve **Red Hat OpenShift Container Platform 4.20** temel alınarak sunulmaktadır.

Program boyunca katılımcılar, Avrupa Birliği Cloud Sovereignty Framework yaklaşımını temel alarak sovereign cloud mimarilerini değerlendirmeyi ve uygulamayı öğrenir. Multitenant clusters-as-a-service yapıları için hosted control plane kullanımı, jurisdiction-aware access control, zero-trust isolation ve gelişmiş cryptographic protection yöntemleri eğitimde öne çıkan başlıklardır.

Katılımcılar ayrıca external key management, network-bound disk encryption, confidential computing ve post-quantum cryptography gibi modern güvenlik yaklaşımlarını sovereign cloud altyapılarına nasıl entegre edebileceklerini uygulamalı olarak öğrenir.

Eğitimin Kuruma Katkısı

DO505, dijital egemenlik gereksinimlerini karşılamak ve multitenant cloud platformları işletmek zorunda olan kurumlar için kritik teknik yetkinlikler kazandırmayı amaçlar.

Hosted control plane isolation, jurisdiction-aware identity and access controls, external key management ve farklı veri durumlarında uygulanan cryptographic protection yöntemleri; kurumların data residency, personnel sovereignty ve cryptographic control gibi düzenleyici gereksinimlere daha güçlü şekilde yanıt vermesine yardımcı olur.

Bu bilgi birikimi aynı zamanda sovereign clusters-as-a-service yapılarının doğrulanabilir jurisdiction garantileriyle sunulmasına katkı sağlar ve mevzuata uyumsuzluk riskinin azaltılmasını destekler.

Eğitimin Katılımcıya Katkısı

DO505 eğitimi, Red Hat OpenShift üzerinde sovereign cloud altyapısı tasarlamak ve işletmek isteyen katılımcılara uygulamalı ve ileri düzey beceriler kazandırır.

Eğitimi tamamlayan katılımcılar multitenant hosted control plane yapıları kurma, SPIFFE ve SPIRE ile zero-trust workload identity uygulama, external key management sistemlerini entegre etme, network-bound disk encryption kullanma ve jurisdiction-aware access control politikaları oluşturma konusunda pratik bilgi edinir.

Bu beceriler enterprise architect, IT security practitioner ve operations engineer rollerindeki profesyonellerin sıkı dijital egemenlik gereksinimlerini karşılayan cloud platformlarını daha güvenli ve kontrollü biçimde tasarlamasına ve işletmesine yardımcı olur.

Building a Sovereign Cloud with Red Hat OpenShift (DO505) Eğitimi

Süre: **5 Gün**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

Önkoşullar

Katılımcıların aşağıdaki bilgi ve deneyimlere sahip olması önerilmektedir:

- Eğitimin mevcut yetkinlik seviyenize uygun olup olmadığını değerlendirmek için Red Hat'in ücretsiz skills assessment aracının kullanılması
- **Red Hat OpenShift Administration II: Configuring a Production Cluster (DO280)** eğitiminin tamamlanmış olması veya self-managed OpenShift cluster yönetimi ve troubleshooting konusunda eşdeğer deneyim
- Identity and Access Management (IAM), encryption, network policy ve firewall gibi temel security kavramlarına aşinalık
- Zorunlu olmamakla birlikte **Multicluster Management with Red Hat Advanced Cluster Management for Kubernetes (DO432)** eğitiminin tamamlanması veya RHACM konusunda eşdeğer deneyim önerilir

Kimler Katılmalı

Bu eğitim özellikle aşağıdaki profesyoneller için uygundur:

- Sovereign landing zone, control plane ve ilgili güvenlik kontrollerini tasarlayan Enterprise Architect'ler
- SOV framework benzeri yasal ve düzenleyici gereksinimleri teknik politikalara dönüştüren IT Security profesyonelleri
- Cryptographic control, identity ve access management konularından sorumlu güvenlik uzmanları
- Sovereign kontrolleri günlük olarak uygulayan ve yöneten IT Operations ekipleri
- Operational resilience süreçlerinden sorumlu SRE'ler
- Red Hat OpenShift ortamlarında sovereign cloud kontrollerini yöneten System Administrator'lar

Neler Öğreneceksiniz

Eğitim kapsamında aşağıdaki konular ele alınır:

- Dijital egemenliğin temel yapı taşlarını tanımlama ve sovereignty hedeflerini multicluster OpenShift mimarisiyle eşleştirme
- Air-gapped ortamlarda sovereign edge cluster'ların devreye alınması
- Hosted control planes kullanarak multitenant isolation mimarisi tasarlama
- Infrastructure management için GitOps yaklaşımını sovereign source of truth olarak konumlandırma
- Jurisdiction-aware identity ve access control politikaları uygulama
- SPIFFE ve SPIRE kullanarak zero-trust workload identity oluşturma
- Cryptographic sovereignty için external key management entegrasyonu
- Network-bound disk encryption ve confidential computing kullanarak data residency gereksinimlerini destekleme
- Post-quantum cryptography tehditlerine hazırlık
- In-jurisdiction backup kullanarak sovereign disaster recovery süreçleri oluşturma

Building a Sovereign Cloud with Red Hat OpenShift (DO505) Eğitimi

Süre: **5 Gün**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

Eğitim İçeriği

1. Sovereign Cloud Operasyonlarına Giriş

Dijital egemenliğin dört temel sütunu incelenir ve Avrupa Birliği Sovereignty Objectives (SOV) yaklaşımı ele alınır.

Red Hat Advanced Cluster Management (RHACM) hub-and-spoke mimarisinin sovereign cloud provider yapıları içindeki rolü değerlendirilir ve multicluster yönetiminin sovereignty hedefleriyle nasıl ilişkilendirildiği açıklanır.

2. Sovereign Boundary Mimarisi Oluşturma

RHACM kullanılarak yeni sovereign clusters-as-a-service tenant cluster'larının sisteme dahil edilmesi ve yönetilmesi ele alınır.

Hosted control plane ve multitenant mimariler üzerinde zero-trust isolation, operational sovereignty ve jurisdiction-aware access control politikalarının uygulanması incelenir.

Bu bölümde sovereign boundary'nin yalnızca fiziksel veya network seviyesinde değil, kimlik, erişim ve operasyon düzeyinde nasıl oluşturulabileceği üzerinde durulur.

3. Sovereign Veriyi Güvenli Hale Getirme

Tenant cluster'lar ve provider workload'ları için gelişmiş cryptographic control yöntemleri uygulanır.

Data-at-rest, data-in-use ve recovery aşamalarında veri gizliliğini korumak amacıyla external key management, network-bound disk encryption ve confidential computing gibi teknolojilerin nasıl kullanılabileceği ele alınır.

Katılımcılar ayrıca post-quantum cryptography risklerine hazırlık ve disaster recovery süreçlerinde verinin ilgili jurisdiction sınırları içinde tutulması konularını inceler.