

MÜHENDİSLİK ÇALIŞMA DOSYASI / 03

Veri sürekliliği ve güvenlik kiti

Rehberleri okuyun, proje sorularını netleştirin ve çalışma tablosunu ekibinizle doldurun.

01 Store & Forward: kesinti tamponunu nasıl boyutlandırırsınız?

Kayıt hızı, kesinti süresi, kayıt boyutu ve toparlanma kapasitesiyle izlenebilir bir ilk tahmin oluşturun.

02 OPC UA sertifikaları: güvenli bağlantı kontrol listesi

Güven listesini, kimliği ve erişim yetkisini ayrı kontrol ederek kalıcı bir devreye alma süreci kurun.

03 Proje çalışma tablosu

Toplantı notları, sorumlular ve kabul kanıtları için ayrılmış alanlar.

13 Eylül 2026 | Türkçe

Bu çalışma dosyası bir planlama yardımcısıdır. Ürün sürümü, plug-in kullanılabilirliği ve lisans kapsamı proje özelinde doğrulanır.

Store & Forward: kesinti tamponunu nasıl boyutlandırırsınız?

Kayıt hızı, kesinti süresi, kayıt boyutu ve toparlanma kapasitesiyle izlenebilir bir ilk tahmin oluşturun.

Tampon bir kapasite kararıdır

Hedef veritabanı veya ağ erişilemediğinde veriyi geçici saklamak sürekliliği destekler. OPC Router Store & Forward bunun için sunulan bir eklentidir; kullanılabilirliği ve davranışı seçilen sürüm ve akışla doğrulanmalıdır. Tampon sonlu disk kapasitesine sahiptir. Güç kaybı, disk arızası, kuyruk sınırı veya yanlış yapılandırma gibi durumlar nedeniyle mutlak sıfır veri kaybı sözü verilmemelidir. Hangi kesintiyi ne kadar süre karşılamak istediğinizi önce belirleyin.

Ham kapasite hesabı

Gerekli ham alan yaklaşık olarak saniyedeki kayıt $\times$ kayıt başına bayt $\times$ kesinti saniyesidir. 100 kayıt/s, 500 bayt/kayıt ve 4 saat kesinti için 720.000.000 bayt, yani yaklaşık 0,67 GiB gerekir. Gerçek depolama; alan adları, indeksler, kuyruk yapısı ve dosya sistemi nedeniyle daha büyük olabilir. Ham değeri ölçülmüş bir ek yük katsayısı ve güvenlik payıyla çarpın. Araçtaki varsayılan katsayı bir ürün garantisi değil, değiştirilebilir planlama varsayımdır.

Kuyruğun boşalmasını hesaplayın

Bağlantı geri geldiğinde yeni veri üretimi devam eder. Hedef saniyede 150 kayıt işleyebiliyor ve kaynak 100 kayıt üretiyorsa geçmiş birikim yalnızca 50 kayıt/s hızla azalır. Dört saatlik 1.440.000 kayıt yaklaşık sekiz saatte boşalır. Hedef hızı kaynak hızına eşit veya daha düşükse birikim tükenmez. Disk kapasitesini tek başına büyütme bu darboğazı çözmez; hedef yazma, toplu işlem ve kaynak örnekleme seçeneklerini inceleyin.

Sahada doğrulanacak davranışlar

Disk doluluk ve en eski bekleyen kayıt yaşı için uyarı eşiği belirleyin. Kuyruk sırasını, yeniden başlatmadan sonra kalan kayıtları ve hedefte mükerrer kayıt davranışını test edin. Kaynak ile hedef sayımlarını karşılaştırın. Yedeklilik ve Store & Forward farklı problemleri çözer; biri diğerinin yerine otomatik geçmez. Üretime geçmeden önce gerçek veri yüküyle kesinti ve toparlanma deneyi yaparak hesaplama varsayımlarını güncelleyin.

Teknik kaynaklar

OPC Router Store & Forward

<https://www.opc-router.com/add-on-store-and-forward/>

OPC UA sertifikaları: güvenli bağlantı kontrol listesi

Güven listesini, kimliği ve erişim yetkisini ayrı kontrol ederek kalıcı bir devreye alma süreci kurun.

Uygulama kimliği ile kullanıcı yetkisini ayırın

OPC UA uygulama sertifikası, bağlantının diğer ucundaki uygulamanın kimliğini doğrulamak için kullanılır. Kullanıcının hangi etiketleri okuyup yazabileceği ise ayrı bir yetki kararıdır. Güvenilen bir uygulamaya bağlanmak, bütün kullanıcıların bütün işlemleri yapabileceği anlamına gelmez. Önce yalnızca gerekli okuma erişimini tanımlayın. Yazma işlemleri için ayrı kullanıcı, açık kapsam ve tesisin değişiklik prosedürünü uygulayın.

Sertifika yaşam döngüsünü yönetin

Sertifika üretimi, dağıtımı, güven listesine eklenmesi, süresi dolmadan yenilenmesi ve iptal edilmesi için sorumlu belirleyin. Sertifika parmak izini güvenilir bir kanaldan doğrulayın. Bir hata kayboldun diye bütün sertifikaları otomatik kabul etmeyin. Sunucu ve istemci saatlerinin senkron olması, geçerlilik kontrolleri ve olay incelemesi için gereklidir. Makine veya hostname değişikliği sonrasında endpoint ve sertifika eşleşmesini tekrar deneyin.

Ağ sınırlarını koruyun

OPC UA güvenliği, tesis ağı tasarımının yerine geçmez. Erişimi gereken sistemlerle sınırlandırın ve kontrol sistemlerini doğrudan internete açmayın. IT/OT sınırındaki veri akışını, güvenlik duvarı kurallarını ve işletim sahipliğini belgeleyin. Bağlantı problemini çözmek için güvenlik modunu kalıcı olarak kapatmak yerine sertifika, endpoint, DNS ve yetki hatalarını ayrı inceleyin. Destek için paylaşılabilecek loglardan parola ve özel anahtarları çıkarın.

Kabul senaryoları ve bakım

Geçersiz sertifika, süresi dolmuş sertifika, yetkisiz kullanıcı ve yanlış endpoint durumlarını test ortamında deneyin. Sistem beklediğiniz şekilde reddetmeli ve anlaşılır bir hata kaydı üretmelidir. Yenileme sonrası bağlantının yeniden kurulmasını da test edin. Özel anahtarların yedeklenmesi, erişimi ve saklanması kurumun güvenlik politikasına göre yönetilmelidir. Devreye alma belgesine sertifika sahibi, son geçerlilik tarihi ve bir sonraki kontrol tarihini ekleyin.

Teknik kaynaklar

OPC UA Security Model

<https://reference.opcfoundation.org/specs/OPC-10000-2/4>

03 / PROJE ÇALIŞMA TABLOSU

Ekibinizle tamamlayın.

Proje / tesis: _____

Tarih / sorumlu: _____

Karar / kontrol	Notlar, sorumlu ve doğrulama
Kayıt/sn / bayt/kayıt	
Kesinti / ek yük / güvenlik payı	
Hedef hız / toparlanma süresi	
Disk ve kuyruk uyarı eşiği	
Sertifika sahibi / yenileme tarihi	
Kesinti ve geri yükleme testi	

Sonraki adım

Açık sorularınızı ve kaynak-hedef sistemlerinizi info@opcturkey.com adresine iletin. Etkileşimli araçlar: opcrouter.com.tr/araclar