**Denetci.org**

**REFERANS İLKELERİ**

# Yedekleme İlkeleri

**Rİ-DAY-1**

Sürüm 1.0 · 11.08.2026

www.denetci.org

# Yedekleme İlkeleri

Yedekleme, veri, yapılandırma ve diğer gerekli sistem durumlarının kayıp, bozulma veya güven kaybı sonrasında güvenilir bir duruma geri getirilebilmesini ele alır. Amaç yalnızca kopya üretmek değil; doğru zamanda, doğru içeriğin, bütünlüğü korunmuş biçimde ve onu gerekli kılan olaydan yeterli ölçüde bağımsız olarak gerçekten geri getirilebildiği bir kurtarma yeteneği oluşturmaktır.

**İlke 1: Yedekleme kopya üretmekten çok geri dönüş kabiliyeti olarak tasarlanmalıdır.**

Başka bir yerde veri bulunması, ihtiyaç anında hizmetin veya verinin geri getirilebileceğini tek başına göstermez. Yedeklemenin değeri nihai olarak kullanılabilir kurtarma sonucundan doğar.

**İlke 2: Yedekleme kapsamı kaybın gerçek etkisinden türemelidir.**

Her varlık aynı biçimde korunmak zorunda değildir; ancak yalnızca en görünür veri kümelerine odaklanmak da yeterli olmayabilir. Koruma, kaybı halinde önemli sonuç doğuracak veri ve sistem durumlarını kapsamalıdır.

**İlke 3: Kurtarma için gereken durum yalnızca ana veriden ibaret kabul edilmemelidir.**

Yapılandırmalar, şemalar, sertifikalar ve başka gerekli unsurlar olmadan veri tek başına kullanılamayabilir. Yedek kapsamı gerçek hizmetin yeniden kurulması için gerekli durumu dikkate almalıdır.

**İlke 4: Yedekleme önceliği veri miktarına göre belirlenmemelidir.**

Küçük bir yapılandırma veya anahtar kümesi çok büyük bir veri arşivinden daha önemli olabilir. Koruma önceliği boyut yerine kaybın oluşturacağı sonuçla ilişkili olmalıdır.

**İlke 5: Yedekleme sıklığı kabul edilebilir gerçek kayıpla ilişkilendirilmelidir.**

Hızla değişen verinin seyrek yedeklenmesi kurtarma sırasında büyük bilgi kaybı oluşturabilir. Yedekleme aralığı teknik kolaylıktan çok ne kadar geçmiş durumun kaybedilebileceğiyle anlam kazanmalıdır.

**İlke 6: Yedeğin hangi zamana ait olduğu kurtarma kararında görünür olmalıdır.**

Bir yedek mevcut olsa bile beklenenden çok daha eski olabilir. “Yedek var” bilgisi, hangi güvenilir duruma dönülebileceğini açıklamak için yeterli değildir.

**İlke 7: Yedekleme başarısı işlemin tamamlandığına değil kullanılabilir çıktıya dayanmalıdır.**

Bir yedek işi teknik olarak çalışmış ancak eksik, bozuk veya erişilemez bir sonuç üretmiş olabilir. Başarı, ihtiyaç anında kullanılabilecek güvenilir bir kurtarma noktası oluştuğunu göstermelidir.

**İlke 8: Yedekleme yeteneğinin kaybı sessiz normal durum gibi görünmemelidir.**

Yeni yedek üretilememesi, kapsamın daralması veya korunan varlıkların değişmesi gerektiğinde anlaşılabilir olmalıdır. Kurtarma kapasitesindeki kayıp yalnızca gerçek olay sırasında fark edilmemelidir.

**İlke 9: Yedekleme kapsamı ortam değiştikçe gerçek varlıklarla birlikte değişebilmelidir.**

Yeni sistemler ve veri kaynakları otomatik olarak korunduğu varsayılmamalıdır; artık gerekli olmayan varlıklar da süresiz olarak yedeklenmeye devam etmemelidir. Yedek kapsamı gerçek hizmet ve saklama ihtiyaçlarını yansıtmalıdır.

**İlke 10: Yedekler içerdikleri asıl veri kadar güvenlik değeri taşıyabilir.**

Yedekler çoğu zaman verinin geniş ve uzun süreli kopyalarını barındırır. Daha seyrek kullanılmaları onların daha düşük hassasiyette veya daha geniş erişime uygun olduğu anlamına gelmez.

**İlke 11: Yedek yönetimi ile yedek içeriğini kullanma yetkisi gerektiğinde ayrıştırılmalıdır.**

Bir kişinin yedekleme sistemini işletmesi bütün yedeklerdeki verileri okuyabilmesini gerektirmeyebilir. Yönetim, geri yükleme, görüntüleme ve silme gibi farklı güçler oluşturdukları etkiye göre sınırlandırılabilmelidir.

**İlke 12: Üretim sistemini kaybettirebilen aynı güven kaybı bütün yedekleri de kolayca kaybettirmemelidir.**

Aynı hesap, yönetim sistemi veya saldırı üretimi ve bütün geri dönüş noktalarını birlikte değiştirebiliyor ya da silebiliyorsa yedekleme gerçek bağımsızlık sağlamaz. Kurtarma yeteneği onu gerekli kılacak olaydan mümkün olduğu ölçüde ayrıştırılmalıdır.

**İlke 13: Coğrafi veya teknik uzaklık tek başına bağımsızlık anlamına gelmemelidir.**

Uzak bir kopya aynı kimlik, sağlayıcı, yönetim veya başka ortak hata alanına bağlı olabilir. Yedek mimarisi görünür mesafeden çok ortak kayıp nedenlerini azaltmalıdır.

**İlke 14: Değiştirilemezlik kullanılan ürün özelliğinin adına değil gerçek değiştirme ve silme yollarına göre değerlendirilmelidir.**

Bir kopyanın “değiştirilemez” olarak tanımlanması bütün ayrıcalıklı veya alternatif yolların gerçekten bunu engellediğini göstermeyebilir. Güvence, saldırganın veya yüksek yetkili kullanıcının fiilî gücü üzerinden değerlendirilmelidir.

**İlke 15: Yedekleri koruyan kriptografik unsurlar da kurtarma zincirinin parçasıdır.**

Yedek güvenli biçimde şifrelenmiş olsa bile gerekli anahtar kaybolmuşsa veri kullanılamaz hale gelir. Buna karşılık anahtarın yedekle aynı kayıp alanında bulunması da korumanın değerini azaltabilir.

**İlke 16: Yedek bütünlüğü yalnızca dosyanın mevcut olmasına dayanarak varsayılmamalıdır.**

Depolama hatası, eksik kopyalama veya daha önce oluşmuş veri bozulması kullanılabilir görünmeyen yedekler oluşturabilir. Yedeğin beklenen içeriği taşıdığı gerektiğinde doğrulanabilmelidir.

**İlke 17: Replikasyon ve anlık görüntüleme otomatik olarak yedekleme ile eşdeğer sayılmamalıdır.**

Bir değişiklik veya bozulma eş zamanlı biçimde diğer kopyalara da yayılabilir. Teknolojinin yedekleme sayılması, kaybedilmiş daha önceki güvenilir duruma geri dönebilme yeteneğine bağlı olmalıdır.

**İlke 18: Sağlayıcı dayanıklılığı kuruluşun kendi kurtarma ihtiyacıyla karıştırılmamalıdır.**

Bulut veya SaaS sağlayıcısı altyapı kaybına karşı koruma sağlayabilir; ancak kullanıcı hatası, kötü niyetli silme veya geçmiş bir veri durumuna dönme gibi ihtiyaçlar ayrı olabilir. Dış hizmetin dayanıklı olması gerekli yedeğin bulunduğunu otomatik olarak göstermez.

**İlke 19: En yeni yedek her zaman en güvenilir kurtarma noktası değildir.**

Bozulma veya saldırı fark edilmeden önce yedeklere taşınmış olabilir. Kurtarma noktası seçimi yalnızca zamansal yakınlığa değil verinin hangi durumda güvenilir olduğuna dayanmalıdır.

**İlke 20: Yedekten geri getirilen sistem kendiliğinden güvenilir kabul edilmemelidir.**

Eski zafiyetler, ele geçirilmiş kimlikler, zararlı durum veya güncelliğini kaybetmiş yapılandırmalar yedekte bulunabilir. Kurtarma işlemi yalnızca veriyi geri getirmek değil ortaya çıkan sistemin yeniden güvenilir olduğundan emin olmak anlamına gelmelidir.

**İlke 21: Geri yükleme işlemi kendi başına yüksek etkili bir güvenlik yetkisidir.**

Bir yedeği üretim üzerine geri döndürmek mevcut veriyi değiştirebilir veya silebilir. Geri yükleme gücü gerçek ihtiyaca göre sınırlandırılmalı ve önemli kullanımları gerektiğinde açıklanabilir olmalıdır.

**İlke 22: Saklama süresi kurtarma değeri ile oluşturduğu veri maruziyetini birlikte dikkate almalıdır.**

Eski yedekler hukuki veya iş ihtiyacı taşıyabilir; fakat aynı zamanda artık gerekli olmayan hassas veri ve geçmiş sırları korumaya devam edebilir. Yedeklerin süresiz saklanması varsayılan güvenlik yaklaşımı olmamalıdır.

**İlke 23: Yedekleme güvencesi gerçek geri yükleme davranışı üzerinden doğrulanabilmelidir.**

Yedekleme raporları, kopya sayısı veya başarılı görev kayıtları tek başına güvence oluşturmaz. Gerekli veri ve sistem durumunun uygun bir kurtarma noktasından, yeterli bütünlükle ve kabul edilebilir sonuçla gerçekten geri getirilebildiği gösterilebilmelidir.