

SQL Change Guard Kurulum Ön Hazırlık Listesi

Bu belge kurulumdan önce kurumun BT, veritabanı ve güvenlik ekiplerine gönderilir. Amacı kurulum günü beklemeyi ortadan kaldırmaktır: sunucu, hesap, sertifika ve güvenlik duvarı talepleri kurum içinde genelde günler sürer. Aşağıdaki maddeler kurulumdan önce hazır olursa kurulum günü yalnız ürünün kurulması ve yapılandırılmasıyla geçer.

Adım adım kurulum, her ayarın açıklaması ve entegrasyonların ayrıntısı Kurulum ve İşletim Kılavuzu'ndadır.

1. Kurulumun genel görünümü

SQL Change Guard üç parçadan oluşur ve kurum ağında çalışır:

Parça	Ne yapar	Nerede çalışır
Web arayüzü	Kullanıcıların tarayıcıdan açtığı ekranlar	IIS üzerinde statik site
API	İş kurallarını çalıştırır, veritabanına yazar, entegrasyonlara bağlanır	IIS üzerinde ASP.NET Core uygulaması
Worker	Zamanlanmış ve kuyruktaki işleri arka planda çalıştırır	Windows servisi

Üçü aynı Windows sunucusunda çalışabilir. Uygulamanın kendi kayıtları SQL Server üzerindeki bir veritabanında durur. Denetim kayıtları aynı veritabanındaki, SQL Server 2022 ile gelen yalnız eklenebilir defter (ledger) tablosunda tutulur.

Ürün kurum içinde çalışır, internet bağlantısı gerekmez. İstisnalar: bulut üzerindeki bir ITSM'e (ServiceNow, Jira Cloud), bulut kimlik sağlayıcısına (Microsoft Entra ID) ya da dışarıdaki bir zaman damgası sunucusuna bağlanılacaksa ilgili adrese HTTPS (443) çıkışı gerekir.

2. Sunucular

Sunucu	En az	Açıklama
Uygulama sunucusu	Windows Server, 4 çekirdek, 8 GB bellek, 20 GB disk	Web arayüzü, API ve Worker bu sunucuda çalışır
Veritabanı sunucusu	SQL Server 2022 veya üzeri, 4 çekirdek, 16 GB bellek, SSD	Uygulama veritabanı. Denetim kayıtları SQL Server 2022 ile gelen yalnız eklenebilir (append-only) defter (ledger) tablosunda tutulur. Defter bütün sürümlerde vardır; Express yalnız pilot ve küçük kurum için uygundur (10 GB sınırı, şifreli yedek yok). Beş yıllık saklama için 10 GB mertebesinde alan yeterlidir. Sunucuda NTP açık olmalıdır

Uygulama sunucusu ile uygulama veritabanı sunucusu aynı yerel ağda olmalıdır.

Uygulama sunucusuna kurulacak yazılımlar:

Yazılım	Neden
IIS (Web Sunucusu rolü)	Web arayüzü ve API burada yayımlanır
.NET 10 ASP.NET Core Hosting Bundle	API'nin IIS'te çalışması için. Paket .NET 10 çalışma zamanını da içerir; Worker aynı çalışma zamanını kullanır
IIS URL Rewrite modülü	Web arayüzündeki doğrudan bağlantıların (ör. e-postadaki ya da ITSM notundaki talep bağlantısı, kurum hesabıyla giriş dönüşü) açılması için. Microsoft'un ücretsiz eklentisidir

API ve Worker ayrı sunuculara da kurulabilir. Bu durumda Worker, ürünün sırlarını (veritabanı bağlantı dizesi, şifreleme anahtarları) açılışta API'den alır; kanıt imzalama özel anahtarı Worker'a gitmez; bu yüzden Worker ile API arasındaki bağlantı HTTPS olmalıdır. Ürün bu bağlantının şifresiz ve uzak bir adresten yapıldığını fark ederse Yönetişim Kurulum Kontrolü ekranında uyarı gösterir.

3. Adresler (DNS)

Web arayüzü ve API için birer adres belirlenmelidir. Bu adresler birkaç ayarda ve web arayüzü paketinde kullanılır, sonradan değişmesi yeniden yapılandırma gerektirir.

Adres	Örnek	Nerede kullanılır
Web arayüzü	https://changeguard.kurum.local	Kullanıcıların açtığı adres; e-posta ve ITSM notlarındaki bağlantılar
API	https://changeguard-api.kurum.local	Web arayüzü, Worker ve kurum hesabıyla giriş bu adresi kullanır

Web arayüzü paketi API adresiyle birlikte hazırlanır. Bu yüzden API adresinin kurulumdan önce kesinleşmesi gerekir.

4. Sertifikalar

Sertifika	Ne için	Zorunlu mu
Web arayüzü ve API adresleri için HTTPS sertifikası	Tarayıcı ile sunucu arasındaki trafik; kurum hesabıyla giriş HTTPS olmadan çalışmaz	Evet
Kurum dizini (LDAPS) sunucu sertifikasının güvenilir olması	Dizine şifreli bağlantı. Kurumun kök sertifikası uygulama sunucusunun güven deposunda olmalıdır	LDAP kullanılacaksa
SIEM toplayıcısının TLS sertifikası	Olayların SOC'a şifreli gönderilmesi	SIEM TLS ile kullanılacaksa
SAML imza sertifikası (.pfx)	Kimlik sağlayıcısı imzalı istek isterse	Yalnız bu durumda

5. Hesaplar ve yetkiler

5.1 Veritabanı hesapları

Hesap	Nerede	Yetki
Uygulama veritabanı hesabı	Uygulama veritabanı	Kurulumu ürünün yapması için (Database:AutoMigrate = true, varsayılan): veritabanında db_owner. Veritabanı önceden boş olarak açılmazsa ürün onu kendisi oluşturur; bu durumda hesaba ayrıca veritabanı oluşturma yetkisi (dbcreator) gerekir. Kurulumu DBA yapacaksa (AutoMigrate = false): DBA kurulum betiklerini uygular, uygulama hesabına db_datareader, db_datawriter ve EXECUTE verilir; hesap ayrıca kanıt defteri rollerine (evidence_api_writer, evidence_worker_writer) eklenir, VIEW LEDGER CONTENT ve evidence şemasında VIEW DEFINITION izni alır. sysadmin gerekmez
Worker veritabanı hesabı (isteğe bağlı)	Uygulama veritabanı	Varsayılan olarak Worker, API ile aynı hesabı kullanır. Ayrı hesap istenirse: db_datareader, db_datawriter, EXECUTE, evidence_worker_writer rolü, VIEW LEDGER CONTENT ve evidence şemasında VIEW DEFINITION. Bu durumda API hesabı yalnız evidence_api_writer rolünde olur; veritabanı, Worker hesabının kullanıcı kararlarını (onay, ret, uzlaştırma kararı) ve giriş olaylarını yazmasını reddeder
Hedef veritabanı hesapları	Yönetilecek her SQL Server, PostgreSQL ve Oracle sunucusu	Onaylanan betiklerdeki işlemleri yapabilecek yetki. Ürün bunlara ek olarak geri alma betiği üretmek ve nesne karşılaştırması için nesne tanımlarını okur (SQL Server'da VIEW DEFINITION). Oracle hesabı ayrıca DBMS_TRANSACTION paketini çalıştırabilmelidir (Oracle'da varsayılan olarak PUBLIC'e açıktır; kurum bu yetkiyi kaldırırsa hesaba GRANT EXECUTE ON SYS.DBMS_TRANSACTION verilir). Ürün bu paketle her bloktan önce ve sonra transaction kimliğini okur. Bu hesaplar ürünün Sunucular

Hesap	Nerede	Yetki
		ekranında girilir, şifreleri şifrelenerek saklanır

Bağlantı dizesi standart bir SQL Server bağlantı dizesidir. SQL Server oturumu önerilir. Windows kimlik doğrulaması kullanılacaksa veritabanı yetkisi hem API'nin IIS uygulama havuzu hesabına hem Worker servis hesabına verilmelidir.

5.2 Windows hesapları

Hesap	Yetki
Worker servis hesabı	Worker klasöründe logs alt klasörüne yazma. Sorgu sonucu dosya klasörüne (QueryResult:OutputPath, ör. D:\SQLChangeGuard\QrFiles) yazma
API uygulama havuzu hesabı (IIS)	API klasöründe logs alt klasörüne yazma. Sorgu sonucu dosya klasörünü okuma (indirme için). Defter özeti klasörüne (6.7) yeni dosya yazma ve okuma. Kanıt imza sertifikasının özel anahtarını okuma

5.3 Entegrasyon hesapları (kullanılacaklar için)

Entegrasyon	Kurumdan istenen hesap	Yetki
Kurum dizini (LDAP / Active Directory)	Okuma yetkili servis hesabı (tam adı ve parolası)	Kişileri ve grupları okuma. Yazma yetkisi gerekmez
Kurum hesabıyla giriş (SSO)	Kimlik sağlayıcısında uygulama kaydı (OIDC) ya da güvenen taraf kaydı (SAML)	Bkz. 6.2
ITSM (ServiceNow, Jira ya da genel REST sağlayıcısıyla ServiceCore gibi diğerleri)	Entegrasyon hesabı	ServiceNow: change_request, incident ve sc_req_item tablolarını okuma, work_notes alanına yazma. Jira: ilgili projelerde görme ve yorum ekleme. Durum değiştirme ve silme yetkisi verilmez
E-posta (SMTP)	Gönderici hesap	E-posta gönderme

6. Kurumdan istenecek bilgiler

Kullanılmayacak entegrasyonların bölümü boş bırakılır.

6.1 Kurum dizini (LDAP / Active Directory)

Bilgi	Örnek
Dizin sunucusunun adı	dc01.kurum.local
Bağlantı türü ve portu	LDAPS 636 (önerilen) ya da StartTLS 389
Kişilerin aranacağı yol (BaseDn)	OU=Calisanlar,DC=kurum,DC=local
Alan adı (NetBIOS) ya da UPN soneki	KURUM ya da kurum.local
Okuma yetkili servis hesabının tam adı	CN=change-guard-okuyucu,OU=Servis,DC=kurum,DC=local
Dizinin hatalı parola kilit eşiği	Ör. 10 deneme. Ürünün kendi kilit eşiği bundan küçük tutulur
Ürün rolleriyle eşlenecek izin grupları	CN=DBA-Ekibi,OU=Gruplar,DC=kurum,DC=local gibi grupların listesi ve her birinin alacağı rol

6.2 Kurum hesabıyla giriş (SSO)

Bilgi	OIDC (Entra ID, Keycloak, Okta)	SAML (AD FS, Entra ID)
Kimlik sağlayıcısının adresi	Authority, ör. https://login.microsoftonline.com/kiraci-id/v2.0	Üstveri adresi, ör. https://adfs.kurum.local/FederationMetadata/2007-06/FederationMetadata.xml
Uygulama kaydı	İstemci kimliği ve istemci sırrı	Güvenen taraf kaydı
Kimlik sağlayıcısına girilecek dönüş adresi	https://API-ADRESİ/api/auth/sso/callback/SAĞLAYICI-ADI	https://API-ADRESİ/api/auth/sso/saml/acs/SAĞLAYICI-ADI
Rol eşlemesi için grup ya da uygulama rolü bilgisi	Entra ID'de uygulama rolleri (önerilen) ya da grup kimlikleri	Rol iddiası
MFA iddiası	Kimlik sağlayıcısı MFA yaptığında hangi iddiayı gönderiyor (Entra ID: amr = mfa)	AuthnContextClassRef (AD FS: http://schemas.microsoft.com/claims/multipleauthn)

SAĞLAYICI-ADI, kurulumda kimlik sağlayıcısına verilecek kalıcı addır (ör. Entra). Kurulumdan sonra değiştirilmez.

6.3 ITSM

Bilgi	Örnek
ITSM ürünü	ServiceNow, Jira Cloud, Jira Data Center, ServiceCore ya da diğer
Adres	https://kurum.service-now.com
Entegrasyon hesabı ve kimlik türü	Kullanıcı adı ve parola; Jira Cloud'da e-posta ve API anahtarı; Jira Data Center'da kişisel erişim anahtarı
Değişiklik kaydı durum adları	Hangi durumlarda iş uygulanabilir sayılır (ServiceNow varsayılanı: Scheduled, Implement); hangi durumlar kapanmıştır
Numara biçimleri	Değişiklik kaydı (CHG0012345), hizmet talebi (RITM0012345), olay kaydı (INC0012345)
Jira'da kayıt tipleri	Değişiklik, olay ve hizmet talebi olarak kullanılan tip adları
Jira'da planlanan zaman alanları	Planlanan başlangıç ve bitiş özel alanlarının kimliği (ör. customfield_10050)
ServiceCore ve diğerleri	Kaydı okuyan API adresi, yanıtaki durum, başlık ve onay alanlarının adı, not ekleme adresi

6.4 SIEM / SOC

Bilgi	Örnek
Toplayıcı adresi ve portu	siem.kurum.local, 6514
Protokol	TLS (önerilen), TCP ya da UDP
Biçim	Rfc5424Json (varsayılan), Cef (ArcSight), Leef (QRadar), Json
Toplayıcının kendi imzalı sertifikası varsa parmak izi	

6.5 E-posta (SMTP)

Bilgi	Örnek
SMTP sunucusu ve portu	smtp.kurum.local, 587
Şifreli bağlantı	Evet ya da hayır
Gönderici hesap, adres ve görünen ad	changeguard@kurum.com.tr, SQL Change Guard

6.6 Zaman damgası (isteğe bağlı)

Bilgi	Örnek
Kurumun RFC 3161 zaman damgası sunucusu	https://tsa.kurum.local/tsr
İnternete çıkış vekil sunucusu (varsa)	http://vekil.kurum.local:8080

6.7 Defter özetleri için değiştirilemez depo

Varsayılan olarak saatte bir veritabanının defter özeti bir dosya olarak (imza açıksa imzalı) bu klasöre yazılır (Evidence:Ledger:DigestOutputPath). Turu Worker başlatır; özeti API alır, imzalar (imza açıksa) ve yazar. Klasör aşağıdaki gibi kilitli bir depodaysa bu dosyalar, veritabanını yönetenlerin sonradan değiştiremeyeceği dış tanık olur; deponun kilidini ürün değil kurum sağlar. Yol boş bırakılırsa dış dosya yazılmaz ve defter yalnız kendi içindeki özetle doğrulanabilir.

Bilgi	Örnek
Klasör yolu (API sunucusundan görülen)	\\worm.kurum.local\changelog-digest
Depo türü	WORM paylaşımı, nesne kilitli depo ya da kurumun arşiv sistemi
Kilit ve saklama süresi	Dosyalar silinemez ve değiştirilemez; saklama süresi veritabanı yedeklerinden uzun
Kim yönetir	DBA ve uygulama sunucusu yöneticisinden farklı bir ekip

Bu klasörde API uygulama havuzu hesabına yeni dosya yazma ve okuma izni yeterlidir (okuma, son özetle sürekliliği kontrol etmek içindir). Worker hesabına bu klasörde izin gerekmez.

7. Kurulumda üretilecek anahtarlar

Aşağıdaki değerler kurulum sırasında kurum içinde üretilir ve ortam değişkeni olarak sunucuya yazılır. Dışarıdan alınmaz, SQL Change Guard ekibine gönderilmez. Nasıl üretildikleri Kurulum ve İşletim Kılavuzu'ndadır.

Değer	Ne işe yarar	Kaybolursa
Oturum imza anahtarı	Kullanıcı oturum jetonlarının imzası	Açık oturumlar düşer, herkes yeniden giriş yapar
Sunucu parolası şifreleme anahtarı	Sunucular ekranındaki veritabanı parolalarının şifrlenmesi	Kayıtlı sunucu parolaları yeniden girilir
Sorgu sonucu paketi anahtarı	Sorgu sonucu dosyalarının parolalarının şifrlenmesi	Eski sonuç dosyalarının parolaları görüntülenemez
Worker anahtarı	Worker'ın API'ye kendini tanıtmayı	Worker çalışmaz; yeni anahtar iki tarafa yazılır
Kanıt imzalama anahtar çifti	Denetim dosyalarının, kayıt paketlerinin, defter özetlerinin ve dönem paketlerinin imzalanması. Özel anahtar ortam değişkeninde değil, Windows sertifika deposunda dışa aktarılamaz olarak tutulması önerilir	İmza açıkken anahtar yoksa kanıt çıktıları üretilmez. Açık anahtar ve parmak izi denetçiye verilir ve saklanır
Kurulum kimliği	Kanıt dosyalarının hangi kurulumdan çıktığını gösterir (ör. KURUM-PROD-01)	Sır değildir, sonradan değiştirilmez

Kanıt imzalama ürünün kod varsayılanında kapalıdır (Evidence:Signing:Enabled = false). İmza kapalıyken kanıt çıktıları imzasız üretilir ve Production olarak tanımlı sunucularda talep çalıştırılmaz. Bu yüzden üretim kurulumunda imza açılır ve anahtar çifti kurulumdan önce hazırlanır.

8. Güvenlik duvarı (port) listesi

Kaynak	Hedef	Port	Amaç	Ne zaman
Kullanıcı tarayıcısı	Web arayüzü adresi	443	Ekranlar	Her zaman
Kullanıcı tarayıcısı	API adresi	443	Web arayüzü API'yi tarayıcıdan çağırır	Her zaman
Worker	API adresi	443	Worker yapılandırmasını ve bazı kararları API'den alır	Her zaman (aynı sunucudaysa yerel)
API ve Worker	Uygulama veritabanı	1433	Uygulama kayıtları	Her zaman
API ve Worker	Hedef veritabanları	1433 (SQL Server), 5432 (PostgreSQL), 1521 (Oracle)	Betik çalıştırma, bağlantı testi, nesne tanımı okuma	Her zaman
API ve Worker	SMTP sunucusu	587 ya da kurumun portu	Bildirim e-postaları	E-posta açıksa
API	Kurum dizini	636 (LDAPS) ya da 389 (StartTLS)	Kimlik doğrulama ve izin eşitlemesi	LDAP kullanılıyorsa
API	Kimlik sağlayıcısı	443	Üstveri ve jeton alma	SSO kullanılıyorsa
Kullanıcı tarayıcısı	Kimlik sağlayıcısı	443	Kurumun giriş sayfası	SSO kullanılıyorsa
API	ITSM	443	Kayıt sorgulama ve not yazma	ITSM kullanılıyorsa
API ve Worker	SIEM toplayıcısı	6514 ya da kurumun portu	Olayların SOC'a gönderilmesi	SIEM açıksa
API ve Worker	Zaman damgası sunucusu	443 ya da 80	Kanıt dosyalarına RFC 3161 zaman damgası	Zaman damgası açıksa
API	Defter özeti deposu	445 (SMB) ya da deponun portu	İmzalı defter özeti dosyalarının yazılması	Her zaman (6.7)

Dışarıdan (ITSM, kimlik sağlayıcısı ya da SIEM tarafından) ürüne gelen bir bağlantı gerekmez. Kimlik sağlayıcısının dönüşü kullanıcının tarayıcısı üzerinden gelir.

9. Kim ne yapar

İş	Sorumlu
Sunucuların açılması, IIS, Hosting Bundle ve URL Rewrite kurulumu	Kurum BT
DNS kayıtları ve HTTPS sertifikaları	Kurum BT
Uygulama veritabanı, hesaplar ve yetkiler	Kurum DBA
Güvenlik duvarı kuralları	Kurum güvenlik ekibi
Dizin servis hesabı, SSO uygulama kaydı, ITSM entegrasyon hesabı	İlgili kurum ekipleri
Web arayüzü paketinin kurumun API adresiyle hazırlanması, lisans dosyası	SQL Change Guard
Defter özetleri için değiştirilemez depo (6.7)	Kurum depolama ya da arşiv ekibi
Dönem paketlerinin teslim alınması ve kaydı	Kurum iç denetimi
Kurulum, yapılandırma ve kurulum sonrası kontrol	Kurum BT ile birlikte SQL Change Guard

Kanıtın bağımsız kalması için en az şu üç rol ayrı kişilerde olmalıdır: DBA, SIEM yöneticisi ve dönem paketini teslim alan iç denetim. DBA, veritabanı sunucusunda işletim sistemi yöneticisi olmamalıdır.

10. Kurulum günü kontrol listesi

- ☐ Uygulama sunucusu hazır: IIS, .NET 10 Hosting Bundle, URL Rewrite kurulu
- ☐ Web arayüzü ve API adresleri DNS'te tanımlı, HTTPS sertifikaları hazır
- ☐ Uygulama veritabanı SQL Server 2022 ya da sonrasında, NTP açık
- ☐ Uygulama veritabanı hesabı ve yetkisi hazır (ve gerekiyorsa boş veritabanı açıldı)
- ☐ Defter özetleri için değiştirilemez depo klasörü hazır, API hesabının yeni dosya yazma ve okuma izni var
- ☐ Kanıt imza sertifikası API sunucusunun sertifika deposunda, özel anahtar okuma izni yalnız API hesabında
- ☐ Worker servis hesabı ve sorgu sonucu dosya klasörü hazır
- ☐ En az bir hedef veritabanı için hesap hazır
- ☐ Güvenlik duvarı kuralları açıldı
- ☐ Kullanılacak entegrasyonların bilgileri (bölüm 6) toplandı
- ☐ Kurulum kimliği belirlendi (bölüm 7)
- ☐ SQL Change Guard lisans dosyası ve web arayüzü paketi teslim alındı