CPB-2026-003

Bulut denetim kaydı 2026: yedi bulut sağlayıcısında yetenekler ve olay modelleri

Yedi bulut sağlayıcısında kontrol düzlemi denetim kaydı, kimlik, saklama, aktarım ve bütünlüğün ortak olay modeliyle dokümantasyona dayalı değerlendirmesi.

SÜRÜM
1.0

YAYIMLANDI
6 Kasım 2026

GÜNCELLENDİ
6 Kasım 2026

ÇEVRİMİÇİ SÜRÜM
https://www.cloudproviderbenchmarks.com/tr/reports/bulut-denetim-kaydi-2026/

İçindekiler

Yönetici özeti

1. Kapsam

2. Sağlayıcı düzeyinde yetenek

3. Özellik değerlendirmesi

4. Ortak olay modeli

5. Sağlayıcılara göre bulgular

6. Alıcılar için öneriler

7. Sonuç

Sınırlamalar

Sürüm geçmişi

Kaynaklar

KISA YANIT

Karşılaştırılan servisler AWS CloudTrail, PortvMind vTrail, Google Cloud Audit Logs ve Azure Activity Log'dur. CloudTrail, Google Cloud Audit Logs ve Azure Activity Log; aktarım ve saklama özellikleriyle birlikte belgelenmiş, varsayılan olarak açık kontrol düzlemi denetim kaydı sunar. vTrail kimlikle ilişkilendirilmiş yönetim işlemlerini kaydeder; saklama, aktarım ve bütünlük özellikleri henüz kamuya açık olarak belgelenmemiştir. DigitalOcean, Vultr ve Hetzner doğrulanmamıştır.

YÖNETİCİ ÖZETİ

Bu rapor AWS, PortvMind Cloud, Google Cloud, Microsoft Azure, DigitalOcean, Vultr ve Hetzner'deki müşteriye yönelik denetim kaydını dokuz nitel özellikle değerlendirir ve PortvMind'ın vTrail olay modelini CloudTrail, Google Cloud Audit Logs ve DMTF CADF ile eşler. Üç büyük bulut sağlayıcısı; varsayılan kontrol düzlemi kaydı, isteğe bağlı veri erişimi kayıtları, saklama ve aktarım sunan olgun servisler belgeler. PortvMind, vTrail aracılığıyla kontrol düzlemi kapsamını, kimlik ve istek meta verisini belgeler. DigitalOcean, Vultr ve Hetzner için müşteriye yönelik bir kontrol düzlemi denetim kaydı kamuya açık dokümantasyondan doğrulanamamıştır.

TEMEL BULGULAR

01 Üç büyük bulut sağlayıcısının tamamı kontrol düzlemi olaylarını varsayılan olarak kaydeder; veri erişimi olayları isteğe bağlıdır ve genellikle ücretlidir.

02 Varsayılan saklama 90 gün (CloudTrail olay geçmişi, Azure Activity Log) veya 400 gündür (Google Admin Activity).

03 Kriptografik bütünlük doğrulamasını yalnızca CloudTrail belgeler; Google ve Azure hedefteki kilitli bucket'lara veya değiştirilemez depolamaya dayanır.

04 vTrail'in alan kümesi kim, ne, ne zaman, nereden ve hangi sonuçla sorularını; ayrıca CloudTrail'in kaydetmediği istek süresi ve ağ geçidi rota kimliklerini kapsar.

05 Kamuya açık denetim kaydı dokümantasyonu, özelliği DigitalOcean, Vultr ve Hetzner'de doğrulamak için yetersizdi.

1. Kapsam

Rapor, yönetim (kontrol düzlemi) aktivitesine ilişkin müşteriye yönelik denetim kayıtlarını kapsar: kim, hangi kaynak üzerinde, ne zaman, nereden ve hangi sonuçla ne yaptı. Bunların üzerine kurulan güvenlik

operasyonu ürünleri (SIEM'ler, tehdit tespiti) kapsam dışıdır. Yöntem: bulut denetimi metodolojisi.

2. Sağlayıcı düzeyinde yetenek

Denetim ve ağ güvenliği yetenekleri, tüm sağlayıcılar

ÖLÇÜT	PORTVMİND	AWS	AZURE	GOOGLE CLOUD
Ağ				
Özel ağlar / VPC Özel CIDR aralığına sahip izole kiracı ağları.	● Var Özel CIDR'lı izole ağlar.	● Var	● Var	● Var
Güvenlik grupları / bulut güvenlik duvarı API ile yönetilen durum bilgili ağ erişim kuralları.	● Var	● Var	● Var	● Var VPC güvenlik du kuralları ve polit
Güvenlik ve denetim				
Kontrol düzlemi denetim kaydı Bulut kaynaklarına yönelik yönetim (API/konsol) işlemlerini kaydeden sağlayıcı servisi.	● Var vTrail (sağlayıcı tarafından sağlanan yetenek bilgisi).	● Var AWS CloudTrail.	● Var Azure Monitor Activity Log.	● Var Cloud Audit Log
Denetim kayıtlarında kullanıcı kimliği Her denetim kaydının işlemi yapan kimliği doğrulanmış kullanıcıyı belirtmesi.	● Var vTrail kimliği doğrulanmış kullanıcı, proje ve kapsamı kaydeder (sağlayıcı tarafından sağlanan bilgi).	● Var	● Var	● Var

3. Özellik değerlendirmesi

Aşağıdaki dokuz özellik, belgelenmiş bir denetim kaydı servisi olan sağlayıcılar için değerlendirilmiştir.

Bulut denetim kaydı servislerinin belgelenmiş özellikleri

ÖZELLİK	VTRAİL PortvMind Cloud	AWS CLOUDTRAİL Amazon Web Services	AZURE MONİTOR ACTİVİTY LOG Microsoft Azure
Kontrol düzlemi denetim kapsamı API veya konsol üzerinden yapılan yönetim işlemlerini (oluşturma, değiştirme, silme) kaydeder.	● Var Bulut yönetim API işlemleri.	● Var Yönetim olayları varsayılan olarak kaydedilir.	● Var Azure Resource Manager yazma/silme/eylem işlemleri.
Kimlik ilişkilendirme Her işlemin arkasındaki kimliği doğrulanmış kullanıcıyı, projeyi/hesabı ve kapsamı belirtir.	● Var Kullanıcı kimliği, kullanıcı adı, proje kimliği ve yetki kapsamı.	● Var userIdentity bloğu (principal, hesap, oturum).	● Var Çağıran ve claim bilgileri.
İstek meta verisi İstek kimliği, HTTP metodu, yol, durum kodu, kaynak IP ve user agent bilgisini yakalar.	● Var İstek kimliği, HTTP metodu, yol, durum, istemci IP, user agent, istek süresi.	● Var eventTime, requestID, sourceIPAddress, userAgent, errorCode.	◐ Kısmi Korelasyon kimliği, işlem, durum ve mevcutsa HTTP istek ayrıntılarında çağıran IP.
Veri düzlemi (veri erişimi) olayları Veri düzeyindeki okuma ve yazmaların (ör. nesne okuma) isteğe bağlı kaydı.	*? Doğrulanmadı*	● Var Veri olayları (ör. S3 nesne düzeyi) isteğe bağlıdır ve ücretlidir.	◐ Kısmi Activity Log'un kendisi değil, kaynak logları ve tanılama ayarlarıyla.
Olay arama ve filtreleme Kullanıcı, zaman aralığı, kaynak veya işleme göre konsol ya da API üzerinden arama.	*? Doğrulanmadı*	● Var Olay geçmişi araması; CloudTrail Lake'te SQL sorguları.	● Var Portal filtreleme ve Log Analytics (KQL).
Yapılandırılabilir saklama süresi Belgelenmiş varsayılan saklama süresi ve uzatma seçenekleri.	*? Doğrulanmadı*	● Var 90 günlük olay geçmişi; S3 trail veya CloudTrail Lake ile daha uzun saklama.	● Var Platformda 90 gün; Log Analytics veya Storage ile daha uzun.
Dışa aktarma ve akış Nesne depolama, log analitiği veya SIEM hatlarına aktarım.	*? Doğrulanmadı*	● Var S3, CloudWatch Logs, EventBridge.	● Var Tanılama ayarlarıyla Log Analytics, Storage ve Event Hubs.
Kayıt bütünlüğü doğrulama Değiştirilmeyi tespit eden kriptografik veya değiştirilemezlik kontrolleri.	*? Doğrulanmadı*	● Var Digest dosyalarıyla log bütünlüğü doğrulama.	◐ Kısmi Aktarım hedefinde değiştirilemez depolama politikaları.
Fiyatlandırma modeli Temel denetim geçmişinin dahil olup olmadığı ve gelişmiş özelliklerin nasıl ücretlendirildiği.	*? Doğrulanmadı*	● Var Olay geçmişi ve yönetim olaylarının bir kopyası ücretsiz; veri olayları ve Lake ücretli.	● Var 90 günlük Activity Log dahil; Log Analytics alımı ücretlidir.
Bilgi kaynağı	Sağlayıcı ekibince sağlandı	Resmî dokümantasyon	Resmî dokümantasyon

4. Ortak olay modeli

Birden fazla sağlayıcının denetim verisini birleştirmek ortak bir model gerektirir. Tablo, vTrail olay modelinin alanlarını CloudTrail, Google Cloud Audit Logs ve CADF ile eşler.

Kavramsal bulut denetim olayı veri modeli

Araştırma dokümantasyonu içindir; üretim denetim kayıtlarını temsil etmez.

ALAN	TİP	AÇIKLAMA	AWS CLOUDTRAİL	GOOGLE CLOUD AUDİT LOGS
event_time	string (RFC 3339)	İşlemin alındığı zaman (UTC).	eventTime	timestamp
request_id	string	Gateway, servis ve kaynak loglarını ilişkilendirmek için benzersiz istek kimliği.	requestID	insertId / operation.id
http_method	string	API çağrısının HTTP fiili (GET, POST, PUT, PATCH, DELETE).	–	httpRequest.requestMethod
full_path	string	Hedef kaynağı belirten istenen API yolu.	eventSource + eventName	protoPayload.methodName / resourceName
http_status	integer	Yanıt durum kodu — işlemin sonucu.	errorCode (on failure)	protoPayload.status.code
client_ip	string (IP)	Çağıranın kaynak IP adresi.	sourceIPAddress	protoPayload.requestMetadata.callerIp
user_agent	string	İstemci yazılımı (konsol, CLI, SDK, Terraform).	userAgent	protoPayload.requestMetadata.callerSupplie
auth_user_id	string	Kimliği doğrulanmış kullanıcının kalıcı kimliği.	userIdentity.principalId	protoPayload.authenticationInfo.principalS
auth_user_name	string	İstek anındaki okunabilir kullanıcı adı.	userIdentity.userName / arn	protoPayload.authenticationInfo.principalE
auth_project_id	string	Token kapsamındaki	recipientAccountId	resource.labels.project_id

ALAN	TİP	AÇIKLAMA	AWS CLOUDTRAİL	GOOGLE CLOUD AUDİT LOGS
		proje (kiracı).		
auth_scope	string	Token'ın yetki kapsamı veya rol bağlamı.	userIdentity.sessionContext	protoPayload.authorizationInfo
service_id	string	İsteği işleyen arka uç bulut servisi (compute, ağ, depolama).	eventSource	protoPayload.serviceName
route_id	string	İstekle eşleşen API gateway rotası.	–	–
request_time	number (ms)	Uçtan uca istek işleme süresi.	–	httpRequest.latency

Boş şablon (JSON)

```
{
  "event_time": "",
  "request_id": "",
  "http_method": "",
  "full_path": "",
  "http_status": null,
  "client_ip": "",
  "user_agent": "",
  "auth_user_id": "",
  "auth_user_name": "",
  "auth_project_id": "",
  "auth_scope": "",
  "service_id": "",
  "route_id": "",
  "request_time": null
}
```

İki vTrail alanı öne çıkar: yalnızca Google Cloud'un `httpRequest.latency` aracılığıyla sunduğu `request_time` (istek süresi) ve API ağ geçidi rotasını tanımlayan, diğer biçimlerde karşılığı olmayan `route_id`. `http_method` da CloudTrail kayıtlarında yer almaz; CloudTrail işlemi `eventSource` ve `eventName` ile ifade eder.

5. Sağlayıcılara göre bulgular

AWS CloudTrail. 90 günlük olay geçmişiyle varsayılan yönetim olayları; S3 ve CloudWatch Logs'a trail'ler; isteğe bağlı, ücretli veri olayları; SQL için CloudTrail Lake; bütünlük için imzalı digest dosyaları.

Google Cloud Audit Logs. Admin Activity her zaman açıktır ve 400 gün saklanır; Data Access çoğunlukla varsayılan olarak kapalıdır; Storage, BigQuery ve Pub/Sub'a sink'ler; kilitli bucket'lar saklama değişikliklerini engeller.

Azure Activity Log. 90 gün boyunca abonelik düzeyinde kontrol düzlemi olayları; tanılama ayarları Log Analytics, Storage ve Event Hubs'a aktarım sağlar; veri düzlemi kaynak kayıtları aracılığıyla.

PortvMind vTrail. Kullanıcı, proje, kapsam ve tam istek meta verisiyle yönetim API işlemleri. Saklama, aktarım, arama, bütünlük ve fiyatlandırma doğrulanmamıştır.

DigitalOcean, Vultr, Hetzner. İncelenen kamuya açık dokümantasyon, müşteriye yönelik bir kontrol düzlemi denetim kaydını doğrulamak için yetersizdi. Dokümantasyon bulunduğunda veya yayımlandığında değerler güncellenecektir.

6. Alıcılar için öneriler

1. Her sağlayıcıdan denetim kaydı saklama süresini, aktarım mekanizmasını ve bütünlük kontrollerini yazılı olarak isteyin.
2. Denetim olaylarını, bir kez yazılabilir korumayla kontrolünüzdeki depolamaya aktarın.
3. Tespit kuralları oluşturmadan önce birden fazla sağlayıcıdan gelen olayları ortak bir şemaya normalleştirin.
4. Bilinen işlemler gerçekleştirip bunların doğru kimlikle ilişkilendirilerek göründüğünü doğrulayarak kaydı test edin.

7. Sonuç

Denetim kaydı büyük bulut sağlayıcıları arasında birbirine yakınsamıştır; daha küçük sağlayıcılar ise belgeledikleri konusunda büyük farklılık gösterir. vTrail, PortvMind Cloud'a ayrıntılı bir kontrol düzlemi olay modeli sağlar; değerlendirmesi, operasyonel özellikleri kamuya açık olarak belgelendiğinde tamamlanacaktır.

Sınırlamalar

- Değerlendirmeler kamuya açık dokümantasyona ve sağlayıcı tarafından sağlanan bilgilere dayanır; hiçbir kayıt hattı test edilmemiştir.
- Özellik erişilebilirliği bölgeye, sürüme veya hesap türüne göre değişebilir.
- vTrail bilgisi sağlayıcı tarafından sağlanmıştır.
- "Doğrulanmadı", özelliğin olmadığı anlamına gelmez; dokümantasyonun yetersiz olduğu anlamına gelir.

Sürüm geçmişi

1.0	6 Kasım 2026	İlk baskı.

Kaynaklar

[1] AWS CloudTrail User Guide — AWS — Resmî dokümantasyon
erişim: 6 Kasım 2026

[2] CloudTrail record contents — AWS — Resmî dokümantasyon
erişim: 6 Kasım 2026

[3] Cloud Audit Logs overview — Google Cloud — Resmî dokümantasyon
erişim: 6 Kasım 2026

[4] Azure Monitor activity log — Microsoft — Resmî dokümantasyon
erişim: 6 Kasım 2026

[5] keystonemiddleware — Audit middleware — OpenStack — Resmî dokümantasyon
erişim: 6 Kasım 2026

[6] DMTF Cloud Auditing Data Federation (CADF) — DMTF — Resmî dokümantasyon
erişim: 6 Kasım 2026

[7] NIST SP 800-92: Guide to Computer Security Log Management — NIST — Resmî dokümantasyon
erişim: 6 Kasım 2026

[8] PortvMind Cloud — PortvMind — Sağlayıcı ekibince sağlandı
erişim: 6 Kasım 2026