PANDUAN PELANGGAN · DBENK CLOUD SEGERA HADIR

AutoOps Cloud tanpa Worker: kondisi dan risiko

Kapan pilihan SSH langsung boleh dipakai, risikonya, siapa bertanggung jawab atas apa, penyiapan yang wajib, dan teks persetujuan yang Anda centang.

VPS publik
satu-satunya tempat pilihan ini boleh dipakai

Daftar IP
port SSH hanya untuk alamat IP DBenk

Persetujuan wajib
dicentang dan dicatat bersama waktunya

Ringkasnya

Tanpa Worker hanya untuk VPS publik. Kunci SSH disimpan terenkripsi di DBenk, port SSH terbuka hanya untuk alamat IP DBenk, dan Anda harus mencentang persetujuan yang dicatat bersama waktunya. Untuk server di jaringan kantor, pakai DBenk Worker.

Status hari ini

DBenk Cloud dan DBenk AutoOps Cloud berstatus **segera hadir**: belum bisa dibeli. Panduan ini menjelaskan cara kerja yang dirancang supaya tim IT Anda bisa menilai dan menyiapkannya. Tanda TERSEDIA berarti sudah bisa dipakai hari ini; DIRANCANG berarti dibuka bersama Cloud.

VERSI
1.0 · 4 November 2026

UNTUK
Pengambil keputusan dan tim IT

VERSI TERBARU
lisensi.dbenk.com/panduan

ISI

Daftar isi

01 Kapan boleh tanpa Worker 3
VPS publik saja

02 Risiko 4
apa yang berbeda dibanding Worker

03 Tanggung jawab bersama 5
DBenk dan pelanggan

04 Penyiapan wajib 6
pengguna, kunci, daftar IP, sshd

05 Kunci dan insiden 7
rotasi, pencabutan, insiden

06 Teks persetujuan 8
sama dengan formulir

Semua panduan DBenk Cloud

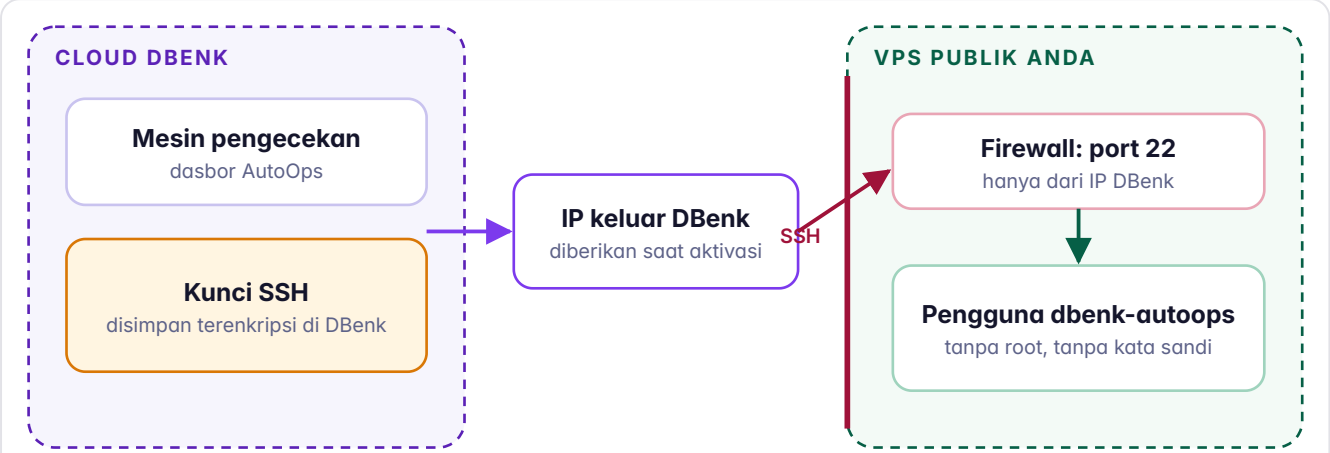
- Panduan DBenk Worker untuk AutoOps Cloud
- AutoOps Cloud tanpa Worker: kondisi dan risiko
- DBenk Cloud: apa yang termasuk

Versi terbaru selalu di **lisensi.dbenk.com/panduan**. Harga dan teks persetujuan di panduan ini berasal dari sumber yang sama dengan halaman harga dbenk.com.

01 KAPAN BOLEH

Kapan AutoOps Cloud boleh tanpa Worker

Cara bawaan AutoOps Cloud adalah DBenk Worker di jaringan Anda. Tanpa Worker adalah pengecualian dengan syarat ketat.



Gambar 1. Tanpa Worker, mesin pengecekan di cloud DBenk menyambung SSH langsung ke VPS publik Anda dari alamat IP keluar DBenk. Kunci SSH disimpan terenkripsi di DBenk, dan firewall VPS hanya menerima port 22 dari alamat itu.

Boleh

- VPS publik (server dengan IP publik di penyedia cloud/hosting) yang memang harus bisa dijangkau dari internet.
- Anda bisa memasang firewall atau security group yang membatasi port SSH per alamat IP.
- Anda bisa membuat pengguna SSH khusus tanpa root di setiap VPS.

Tidak boleh

- Server di jaringan kantor, LAN, atau di belakang NAT: pakai DBenk Worker.
- Membuka port SSH ke seluruh internet supaya DBenk bisa masuk.
- Memakai pengguna root atau kunci yang juga dipakai orang/sistem lain.

Pilihan ini dipilih di formulir minta akses DBenk Cloud dan baru berlaku setelah Anda mencentang persetujuan di halaman 8. Teks, versi, sidik (sha256), dan waktunya disimpan bersama permintaan Anda dan dicatat di data pelanggan Anda di Konsol DBenk.

02 RISIKO

Risiko yang perlu Anda terima

Ini bukan cara yang kami sarankan. Daftar ini menjelaskan apa yang berbeda dibanding memakai DBenk Worker.

RISIKO	ARTINYA	PENGURANGAN
Kunci SSH di luar jaringan Anda	Kunci privat untuk VPS Anda disimpan di DBenk (terenkripsi). Bila sistem DBenk dibobol, kunci itu ikut terancam.	Kunci khusus per pelanggan, terenkripsi, hanya dipakai mesin pengecekan; pengguna berhak minimum; rotasi dan pencabutan (halaman 7).
Port SSH terbuka ke internet	Port 22 VPS harus menerima koneksi dari alamat IP DBenk. Salah atur firewall bisa membuka port ke semua orang.	Daftar IP yang diizinkan, login kunci saja, `AllowUsers`, fail2ban atau sejenisnya.
Ketergantungan pada alamat IP DBenk	Bila alamat IP keluar DBenk berubah, aturan firewall Anda perlu diperbarui.	Perubahan diumumkan lebih dulu lewat e-mail; alamat lama tetap jalan selama masa peralihan.
Penyalahgunaan hak	Siapa pun yang memegang kunci bisa memakai hak pengguna `dbenk-autoops`.	Tanpa root, tanpa sudo bawaan; aksi pengubah hanya bila Anda izinkan per server; semua aksi tercatat.
Jalur lewat internet	Lalu lintas SSH melewati internet publik, bukan jaringan dalam.	SSH terenkripsi; sidik jari host dipatok sejak sambungan pertama, perubahan ditolak sampai Anda konfirmasi.

Lebih aman: pakai DBenk Worker

Worker tidak butuh port masuk dan kunci SSH tetap di jaringan Anda. Bila nanti Anda punya satu server Linux yang selalu menyala, pindah ke Worker kapan saja; panduannya: Panduan DBenk Worker untuk AutoOps Cloud.

03 TANGGUNG JAWAB

Matriks tanggung jawab bersama

Siapa mengurus apa saat AutoOps Cloud menyambung langsung ke VPS Anda.

TANGGUNG JAWAB	DBENK	PELANGGAN
Keamanan kunci SSH yang disimpan di DBenk (enkripsi, akses, pencatatan)	●	—
Keamanan mesin pengecekan dan alamat IP keluar DBenk	●	—
Memberi tahu Anda bila ada insiden yang menyangkut kunci Anda	●	—
Mengumumkan perubahan alamat IP keluar lebih dulu	●	—
Membuat dan membatasi pengguna `dbenk-autoops`	—	●
Firewall/security group: port SSH hanya untuk IP DBenk	—	●
Pembaruan keamanan OS dan SSH di VPS	—	●
Memutuskan aksi pengubah mana yang diizinkan per server	—	●
Mencabut akses (hapus kunci publik) saat dibutuhkan	—	●
Menghapus kunci tersimpan setelah diminta atau setelah langganan berakhir	●	—
Menyimpan catatan persetujuan ini	●	●

● = bertanggung jawab. Pembagian ini sama dengan poin (4) di teks persetujuan.

04 PENYIAPAN

Penyiapan yang wajib

Lakukan di setiap VPS sebelum menambahkannya ke AutoOps Cloud.

1 Pengguna SSH khusus berhak minimum

```
sudo useradd --create-home --shell /bin/bash dbenk-autoops
sudo passwd --lock dbenk-autoops
sudo install -d -m 700 -o dbenk-autoops -g dbenk-autoops /home/dbenk-autoops/.ssh
```

2 Kunci publik DBenk, dibatasi

Kunci publik khusus untuk Anda tampil di dasbor setelah aktivasi. Tambahkan dengan pembatasan supaya kunci hanya bisa dipakai dari alamat DBenk dan tanpa penerusan:

```
from="<IP-DBenk-1>,<IP-DBenk-2>",no-agent-forwarding,no-port-forwarding,no-X11-forwarding
ssh-ed25519 AAAA… dbenk-autoops-cloud
```

Simpan di `/home/dbenk-autoops/.ssh/authorized_keys` (600, milik `dbenk-autoops`).

3 Daftar IP yang diizinkan

Alamat IP keluar DBenk: **diberikan saat aktivasi**. Izinkan port SSH hanya dari alamat itu, di firewall VPS dan di security group penyedia bila ada:

```
sudo ufw allow from <IP-DBenk-1> to any port 22 proto tcp
sudo ufw allow from <IP-DBenk-2> to any port 22 proto tcp
# pastikan akses admin Anda sendiri tetap ada sebelum menutup yang lain
```

4 Perketat sshd

```
# /etc/ssh/sshd_config.d/dbenk.conf
PasswordAuthentication no
PermitRootLogin no
AllowUsers dbenk-autoops <admin-anda>
# lalu: sudo sshd -t && sudo systemctl reload ssh
```

05 KUNCI DAN INSIDEN

Rotasi, pencabutan, dan penanganan insiden

Rotasi kunci

1. Minta kunci baru di dasbor (**Server › Kunci › Buat kunci baru**) atau lewat dukungan.
2. Tambahkan kunci publik baru di setiap VPS, di samping yang lama.
3. Tekan **Uji sambungan**; setelah semua berhasil, hapus kunci lama dari VPS.
4. Kunci lama dihapus dari penyimpanan DBenk dan tercatat di riwayat.

Kami menyarankan rotasi setiap 90 hari dan segera setelah ada orang yang keluar dari tim yang memegang akses admin.

Mencabut akses

- **Seketika, oleh Anda:** hapus baris kunci DBenk dari `authorized_keys`, atau tutup aturan firewall untuk IP DBenk.
- **Penghapusan di DBenk:** minta lewat dasbor atau dukungan; kunci tersimpan dihapus dan Anda menerima konfirmasi tertulis.
- Saat langganan berakhir, kunci tersimpan dihapus.

Bila terjadi insiden

SITUASI	YANG ANDA LAKUKAN	YANG DBENK LAKUKAN
Anda curiga VPS dibobol	Cabut kunci DBenk dan tutup port SSH; amankan VPS; kabari kami.	Menghentikan pengecekan ke VPS itu, mengirim riwayat aksi AutoOps ke VPS itu untuk penyelidikan Anda, membuat kunci baru bila diminta.
Insiden di sisi DBenk	Ikuti petunjuk di pemberitahuan; cabut kunci bila diminta.	Menonaktifkan kunci yang terdampak, memberi tahu Anda tanpa menunda, menjelaskan apa yang terdampak, dan menerbitkan kunci baru.
Aksi tak terduga di log	Laporkan waktu dan servernya.	Mencocokkan dengan catatan audit AutoOps dan menjelaskan asal aksinya.

06 PERSETUJUAN

Teks persetujuan

Teks ini sama persis dengan yang Anda centang di formulir minta akses. Bila teks berubah, versinya naik dan persetujuan perlu diberikan ulang.

> Saya memilih DBenk AutoOps Cloud TANPA DBenk Worker untuk server VPS publik saya dan memahami kondisinya: (1) kunci SSH untuk server ini disimpan terenkripsi di DBenk dan dipakai hanya oleh mesin pengecekan AutoOps; (2) port SSH server saya terbuka untuk alamat IP keluar DBenk (diberikan saat aktivasi) dan saya membatasi akses ke alamat itu saja; (3) saya membuat pengguna SSH khusus dengan hak minimum (bukan root), dan perubahan hanya jalan bila saya izinkan per server; (4) DBenk bertanggung jawab atas keamanan kunci dan mesin pengecekan di cloud DBenk, saya bertanggung jawab atas server, pengguna, dan firewall saya; (5) saya bisa mencabut akses kapan saja dengan menghapus kunci publik DBenk dari server dan meminta penghapusan kunci di DBenk.

Versi	`autoops-ssh-langsung/1`
Sidik teks (sha256)	`71f32927b305a6de41eeebc7522863ac2b6280325f9881f64d41fd4177202e36`
Yang dicatat	teks dan bahasanya, versi, sidik, waktu centang, nama, e-mail, dan perusahaan; dicatat bersama permintaan dan di data pelanggan di Konsol DBenk
Menarik persetujuan	pindah ke DBenk Worker atau hentikan pemantauan VPS itu; kunci tersimpan dihapus

Sidik dihitung dari teks di atas (UTF-8) sehingga siapa pun bisa memastikan teks yang disetujui tidak berubah.