Administratörsmanual — AI-boxen

Administratörsmanual

Self Production · selfproduction.se
Byggd 2026-11-01 ur manualer/administratorsmanual.md#A
Klassning: Kund

Administratörsmanual — AI-boxen

Version 1.6 · 25 oktober 2026 · gäller AI-boxen 1.74.0

Manualen är skriven för:

- **Del A** är till kundens administratör, alltså den hos kunden som äger boxen. Den förutsätter att du kan logga in på en Linuxserver med ssh, men inte att du känner till hur Self Production arbetar.

Innehåll

Del A — Kundens administratör

- A1. Boxen i korthet
- A2. Logga in på maskinen
- A3. Kommandot `aibox`
- A4. Läget och versionerna
- A5. Konton
- A6. Sidan AI-agenter (via kontrollpanelen)
- A7. Mina projekt (via boxens länkar)
- A8. Uppdateringar
- A9. Säkerhetskopior
- A10. Brandväggen och egna regler
- A11. Tunneln
- A12. Nåbar utifrån (`aibox molnet`)
- A13. Spara och driftsätta ett projekt
- A14. Publicera en app
- A15. Städa i git-servern
- A16. Supportdörren
- A17. Hemringningen
- A18. Loggar och felsökning
- A19. Chatten: byggrader och hemsidor
- A20. Post till boxen
- A21. Avdelningar
- A22. Molnkonton
- A23. Tokenmätningen
- A24. Lokal driftövervakning
- A25. Sårbarhetsbevakning och provet av kopiorna (1.84.0)

DEL A — Kundens administratör

A1. Boxen i korthet

AI-boxen är en Ubuntu-server eller en Mac (Apple Silicon) i ert eget nät, eller en virtuell maskin som Self Production har hand om åt er i Azure eller i Arboga Pilotmiljö. Boxen väljs på tre sätt: var den står (virtuell eller on prem), vilken maskin (Ubuntu Server 26.04 LTS eller macOS) och användarläge (**Vanlig box** eller **Fleranvändare**, se A5). NVIDIA-grafikkort används om maskinen har ett och är inget val. På macOS finns ingen lokal modellmotor som standard; modellerna körs via era egna konton eller en modellserver. Tabellen visar tjänsternas interna portar; webbgränssnitten öppnas via kontrollpanelens HTTPS-länkar, inte direkt via port 3000/8080/8090/8091/8092:

Port	Tjänst	Inloggning
22	ssh till maskinen	kontot `ai`
2222	git över ssh (git-servern)	ert git-konto
3000	git-servern (Forgejo), webbgränssnitt	ert git-konto
8080	chatten (Open WebUI)	ert chattkonto
8090	sidan AI-agenter (lägessidan)	chattens administratörskonto
8091	Mina projekt: filerna i projekten och kunskapen, och apparna	boxens konto
8092	apparna i Mina projekt	enligt appen
9000–9099	appar ni själva driftsätter	enligt appen

Modellmotorn (Ollama, port 11434) och kodsandlådan (port 8000) lyssnar bara på maskinen själv och går inte att nå från nätet. Det är med avsikt, eftersom ingen av dem har inloggning.

Standardbrandväggen tillåter SSH, git över SSH, HTTP/HTTPS och appportarna 9000–9099 från privata nät. De interna webbportarna är bundna till loopback sedan 1.51.0; nginx förmedlar åtkomsten via HTTPS och boxens inloggning. Nya boxar från 1.69.0 har tunneln på från leverans. Ni kan stänga av den; uppgraderade boxar behåller tidigare val. Varje app publicerar ni separat (A14).

Inställningarna står i `/etc/ai-boxen/box.conf`. Installern läser filen och skriver om den vid varje körning. Värden som installern känner till följer med till nästa version.

Kundportalen och kontrollpanelen

Från 2026-10-18 gör ni boxens inställningar i **boxens kontrollpanel**, inte i kundportalen. Kundportalen (selfproduction.se/portal) har menyn **Mina boxar · Tjänster och kostnader · Hjälp och support**, och varje box har ett kort med läget, larmen, **Öppna kontrollpanelen**, aktiveringen av ert konto (A5) och det Self Production levererar för boxen: säkerhetskopiornas nivå och arkiv, uppdateringarna och den automatiska uppdateringen, adressnamnet och publiceringen, och granskningarna. Under I kontrollpanelen på kortet leder en länk per del direkt till kontrollpanelens `https://<kontrollpanelen>/`

`installningar/<del>` – Agenter och modeller, Användare på boxen, Om verksamheten, Åtkomst utifrån, Säkerhetskopior, Box och uppdateringar, Systemtjänster, SSH-nycklar, Program och katalog och Anslutna molnkonton.

En box som kör en äldre version har delen kvar i portalen under **Äldre box – inställningar här tills den uppdaterats**: Användare på boxen tills boxen kör 1.70.0, de andra delarna tills den kör 1.59.0. Där den här manualen säger "i portalen under …" om en sådan del gäller det alltså en äldre box; på en nyare box finns samma del, med samma namn, i kontrollpanelen.

A2. Logga in på maskinen

Logga in som användaren `ai`:

```
ssh ai@<boxens-adress>
```

Logga inte in som root. På boxar som installerats från Ubuntus moln-image (alla virtuella boxar) är root spärrat. Ubuntu skriver då "Please login as the user ai", väntar tio sekunder och kopplar ner. Det kan se ut som att maskinen hänger, men det gör den inte.

Kontot `ai` får använda sudo utan lösenord, alltid (från 1.40.0, raden ligger i `/etc/sudoers.d/ai-boxen`). Det gäller också på en fysisk box där installationen satt ett lösenord på kontot; agenterna i chatten arbetar som `ai` och måste kunna driftsätta och publicera det de byggt. Kommandon som ändrar systemet körs med `sudo aibox …`.

Boxens adress i ert nät står i kundportalen på boxens kort, under Kontrollpanelen. Ni kan också se den på boxens egen skärm, om maskinen har en.

A3. Kommandot `aibox`

Med `aibox` gör ni allt som har med boxen att göra. Kör det här för att se alla kommandon:

```
aibox hjalp
```

Kommando	Vad det gör	sudo
`aibox status`	visar vad som kör och vad som saknas	nej (med sudo syns också hur gammal kopian är)
`aibox versioner`	jämför de versioner utgåvan låser med det som faktiskt är installerat	nej
`aibox logg [antal rader]`	visar installationsloggen (40 rader om inget annat anges)	nej
`aibox fraga "…"`	ställer en fråga till boxens standardmodell	nej
`aibox agent [katalog]`	startar aider i ett projekt	nej
	söker i boxens kunskapsindex, eller indexerar om	nej

Kommando	Vad det gör	sudo
`aibox kunskap sok "…"` / `indexera` / `status`		
`aibox butik [kategori]`, `aibox visa <projekt>`, `aibox hamta <projekt>`	låter er bläddra i appbutiken och hämta ett projekt eller en avdelning till `~/projekt/` (paket som ingår i abonnemanget hämtas med boxens nyckel)	nej
`aibox avdelning [lista|kor X:Y|installera X|av X|pa X]`	avdelningarna: roller och rutiner (A21)	`av` och `pa` ja
`aibox post [lista|hamta]`	kundens post från `<alias>@box.selfproduction.se` i `~/post` (A20)	`hamta` ja
`aibox molnkonto …`	kontona hos AWS, Azure och Viploy för agenterna: `lista`, `satt`, `prova`, `ta-bort` (A22)	ja
`aibox sajt [lista|skapa|stang]`	hemsidor skapade från chatten (A19)	ja
`aibox kopiamal …`	egna kopiamål: USB-disk, filserver, SFTP, S3, Azure Blob (A9)	ja
`aibox tokens`	hur mycket agenterna använt modellerna (A23)	ja
`aibox modeller [lista]`, `aibox modeller hamta <namn>`	visar boxens lokala modeller eller hämtar en ny	nej
`aibox hemlighet [nyckel]`	visar nycklarna i agenternas vault, eller skriver ut ett värde	nej
`aibox spara <projekt>`	sparar projektet i boxens git-server	se A13
`aibox konton …`	hanterar konton i chatten och git-servern	ja
`aibox modellserver …`	hanterar modellservrarna boxen får använda	`lista` och `lage` nej, resten ja
`aibox uppdatera [kolla|aterga]`	uppdaterar boxen (`kolla` behöver inte sudo)	ja
`aibox sakerhetskopia [lista|<mål>]`	tar en kopia nu, eller listar kopiorna	ja
`aibox aterstall <fil>`	återställer från en kopia	ja
`aibox aterstall --extern <box-id>`	hämtar tillbaka en död boxs kopia från kopian utanför huset	ja
`aibox aterstall --mal <id> [--fran <box-id>]`	läser tillbaka senaste kopian ur ett eget kopiamål	ja
`aibox extern nyckel|status`	visar återställningsnyckeln och läget för kopian utanför huset	ja
`aibox tunnel [visa|ner]`	startar tunneln, visar läget eller tar ner den	ja

Kommando	Vad det gör	sudo
`aibox molnet [på|av]`	gör boxens egna tjänster nåbara utifrån	ja
`aibox driftsatt <projekt>`	driftsätter ett projekt	ja
`aibox publicera <projekt>`	ger en app en publik adress (flera appar, var och en med egen adress); `--av [projekt]`, `--huvud <projekt>`, `--visa`	ja
`aibox repon [ta-bort X|papperskorg]`	listar och städar repon i git-servern	ja (kommandot tar sudo själv)
`aibox support [på|av]`	öppnar eller stänger supportdörren	ja
`aibox hemringning [visa]`	skickar ett livstecken nu, eller visar vad som senast skickades	`visa` nej, att skicka ja
`aibox uppdrag [visa]`	hämtar det som beställts i portalen nu, utan att vänta på nästa varv	ja
`aibox oidc`	räknar om inloggningen "boxens konto" (se A5)	ja
`aibox chattverktyg`	kopplar in chattens verktyg (git-servern och Boxens kunskap) igen	ja
`aibox vm …`	hanterar virtuella maskiner på er egen virtualiseringsvärd (driftsmålet `vm`, bara Linux)	ja

Exempelprojekten i `~/projekt/` läggs bara vid den första installationen (markören är `/var/lib/ai-boxen/exempelprojekt-lagda`). Ett exempel ni tar bort kommer alltså inte tillbaka vid nästa uppdatering. Vill ni ha fler, eller ett borttaget tillbaka, hämtar ni dem med `aibox butik` och `aibox hamta <projekt>`.

A4. Läget och versionerna

```
sudo aibox status
```

Kommandot visar en bock eller ett kryss för varje tjänst: modellmotorn, chatten, git-servern, kodsandlådan, aider, Claude Code, Claude Code i chatten, docker, lägessidan och appbutiken. Under bockarna står modellerna, antal projekt, ledigt diskutrymme, grafikkortet (om maskinen har ett) och vilken version boxen kör. Om en nyare version finns står det också där, tillsammans med hur ni uppdaterar. Sist visas när boxen senast hörde av sig och hur gammal den senaste säkerhetskopian är.

Kör ni utan `sudo` visas inte kopians ålder, eftersom backupkatalogen bara kan läsas av root.

```
aibox versioner
```

Kommandot jämför komponenterna (Open WebUI, Forgejo, Open Terminal, Ollama, cptr, Claude Code, aider, uv och Node) med de versioner utgåvan låser. Avviker en rad har installern inte körts sedan den ändrades. Då rättar ni det så här:

```
sudo bash /opt/ai-boxen/installer/install.sh
```

A5. Konton

Chatten och git-servern har var sitt kontoregister. Rätten att chatta är alltså inte samma sak som rätten att pusha kod. Lägessidan på lägessidan släpper bara in den som är **administratör i chatten**.

Det första kontot

Kundens administratörskonto skapas av portalen. När boxen ringt hem första gången läggs ett kontouppdrag i kön för varje aktivt portalkonto hos kunden: administratör i chatten och git-servern, med kundens e-postadress från portalen och ett slumpat lösenord som ingen ser (från 1.70.0 inget lösenord alls). Kunden sätter sitt eget på boxen med **Aktivera ert konto på boxen** i portalen (från 1.70.0, se Aktivering och återställning nedan), på en äldre box i portalen under **Användare på boxen → Nytt lösenord**, och får mejlet "Boxen är igång" med det som nästa steg. Finns det redan konton i chatten läggs inget. På en box hos oss öppnas chatten och Mina projekt över internet av sig själva så fort kontot finns.

Det går alltså inte längre att "ta" administratörsplatsen genom att vara först till adressen: platsen är upptagen innan någon hunnit dit. Saknas kontot ändå (till exempel för att kunden saknar portalkonto) skapar ni det själva, i kontrollpanelen eller på maskinen (nedan).

I kontrollpanelen (rekommenderas)

Öppna kontrollpanelen och välj **Inställningar → Användare på boxen**. Där skapar ni konton, ändrar roller och tar bort konton, och lösenordet sätts på boxen. På en box före 1.70.0 görs det i stället i kundportalen, under **Äldre box → Användare på boxen** på boxens kort. Under **Beställ** väljer ni där vad som ska göras:

- **Skapa konto**: ange e-post, namn, roll (Medlem eller Administratör) och tjänster (Chatten, Git-servern), och på en box före 1.70.0 lösenord (minst 12 tecken). Från 1.70.0 skapas kontot utan lösenord och aktiveras med en länk (nedan).
- **Ändra roll**
- **Ta bort konto**
- **Nytt lösenord** (bara en box före 1.70.0): ersätter lösenordet i både chatten och git-servern.

Tryck **Skicka till boxen**. Boxen hämtar beställningen inom ungefär en minut. Lösenordet passerar Self Productions server på vägen till boxen, men sparas inte där. Det försvinner ur beställningen så fort boxen har kvitterat den.

Sidan visar också **vilka** konton boxen har: en tabell med e-post, namn, roll och tjänster (från 1.40.0). Boxen rapporterar listan i hemringningen, så den är som den var vid senaste hemringningen. Lösenord står aldrig med, och boxens systemkonton (`aibox`, `agent`) och chattens interna adresser (`@box.invalid`) listas inte. En box före 1.40.0 rapporterar bara antal, och då säger portalen det. På maskinen visar `sudo aibox konton` kontona.

Inget tak på personkonton. Varken Vanlig box eller Fleranvändare begränsar antalet konton (förr satte storleken ett tak, men det finns inte längre). En person är en e-postadress i chatten eller git-servern; boxens servicekonton räknas inte. Det gäller från box 1.78.0; äldre boxar har kvar taket (liten 2, mellan 3) tills de uppdaterats. På en Vanlig box har alla konton full åtkomst, så bjud bara in dem ni litar på fullt ut. Kollegor som bjuds in till en app i Mina projekt (A7) har inget konto på boxen.

Aktivering och återställning (1.70.0)

Från 1.70.0 väljs lösenordet till ett konto på boxen PÅ BOXEN, och det passerar aldrig Self Productions server.

- **Första inloggningen.** På boxens kort i kundportalen (Ert konto på boxen, och i Kom igång) trycker personen **Aktivera ert konto på boxen** (mer än tio minuter efter inloggningen i portalen frågas lösenordet igen först). Portalen visar en länk en enda gång, `https://kontrollpanel-<namn>.box.selfproduction.se/aktivera#…` (eller `portal-<box-id>.box…` utan adressnamn). Länken gäller i 24 timmar och en gång, och fungerar när boxen hämtat uppdraget (portalen visar "klar att använda", normalt inom en minut). På sidan väljer personen lösenord, minst 12 tecken, och kan lägga till tvåsteg eller en passkey. Utan åtkomst utifrån pekar länken på LAN-namnet `<box-id>.lan.selfproduction.se` och går bara att öppna i kundens nät. En passkey för LAN-namnet läggs till därifrån.
- **Glömt lösenordet.** Samma knapp igen: en ny länk ersätter den gamla.
- **Återställ åtkomst** för en annan administratör på boxen: knappen på personens rad under Återställ åtkomst för någon annan på boxens kort. Den används också för första länken till en administratör som lagts till, eftersom konton från 1.70.0 skapas utan lösenord. Medlemmar återställs inte från portalen: boxens administratörer hjälper dem i kontrollpanelen under **Användare på boxen**. Den som beställer skriver sitt eget lösenord till portalen igen (och koden ur appen om portalkontot har tvåsteg). Länken ges till personen och bara till den. Boxen loggar ut personens sessioner och visar boxens andra administratörer en banderoll så länge länken är obrukad (uppdraget bär `bestallare: portaladmin`); hos oss står den på kundkortet.
- **Tvåsteg och AD.** Har kontot tvåsteg byter länken bara lösenordet; koden ur appen behövs fortfarande. På en Fleranvändare-box med AD vägrar boxen länken för konton som kommer ur AD, och portalen säger att lösenordet byts i AD.
- **Inga lösenord i kön.** Från 1.70.0 skapas kontot vid första kontakten utan lösenord, och kundportalen har ingen **Nytt lösenord**; boxens kö vägrar lösenord i klartext.
- **Bromsar.** Fem länkar per box och person och timme. Den som skriver fel lösenord räknas mot samma broms som inloggningen i portalen.
- Boxen sparar bara en hash av länkens token, en per konto. Portalen har token bara i uppdraget, tills boxen kvitterat det (eller det ångrats, eller fyra dygn gått).

Partnerns konton (1.72.0)

Har kunden köpt boxen genom en partner (en återförsäljare) får partnerns personer var sitt administratörskonto på boxen, från leveransen.

- **Vilka.** Ett konto per person hos partnern som har ett aktiverat konto i partnerrummet. Kontona är märkta Partner: <företag> i kontrollpanelen under **Användare på boxen**, och står på boxens kort i portalen under **Partnerns åtkomst** med sedan när, aktiverat och pausat.
- **Vad de kan.** Samma som en administratör, med ett skydd: ett partnerkonto kan inte ta bort, sänka eller pausa kundens egna administratörer. Partnerkonton räknas inte mot taket på personkonton.

- **Pausa och ta bort.** Kunden pausar ett partnerkonto (det kan inte logga in, inte heller i git-servern, och loggas ut direkt) eller tar bort det i kontrollpanelen under **Användare på boxen**. Ett borttaget konto kommer inte tillbaka av sig självt.
- **Aktivering.** Partnern aktiverar sitt eget konto i partnerrummet med en engångslänk (Aktivera ert konto på boxen) och väljer lösenordet på boxen. **Återställ åtkomst** på boxens kort gäller inte partnerns konton.
- **När partnern slutar.** När en person slutar hos partnern, partnerskapet avslutas, kunden byter partner eller boxen flyttas till en annan kund tar Self Production bort kontona genom kön; kunden som byter partner (eller får boxen) får den nya partnerns konton. Boxen tar bara bort ett konto som verkligen är partnerns. Bekräftar boxen inte borttagningen försöker vi igen, och efter ett dygn syns den på partnerns sida i kontoret.
- **Kundens beslut står kvar.** Ett partnerkonto som kunden tagit bort eller pausat på boxen läggs inte dit igen av sig självt. Vill kunden ha det tillbaka trycker personalen **Tillåt igen** under Kundens beslut på boxarna på partnerns sida i kontoret. Läggs partnerns konton på boxen efter leveransen får kunden notis och brev.
- **Äldre boxar och befintliga kunder.** Gäller boxar med AI-boxen 1.72.0 eller senare som levererats efter att partnerkontona infördes (2026-10-18). Befintliga kunder med partner får dem först efter besked.

På maskinen

```
sudo aibox konton                                          # listan, och startlösenord som inte lä
sudo aibox konton skapa anna@exempel.test "Anna Andersson" medlem chatt,git
sudo aibox konton andra anna@exempel.test admin
sudo aibox konton ta-bort anna@exempel.test chatt,git
sudo aibox konton glom anna@exempel.test                   # kasta startlösenordet när det lämnats
```

`skapa` behöver alla fyra värden: e-post, namn, roll (`admin` eller `medlem`) och tjänster (`chatt`, `git` eller `chatt,git`). Boxen slumpar ett startlösenord och sparar det bara i `/etc/ai-boxen/konton/` (läsbart enbart för root). Läs det med `sudo aibox konton`, ge det till personen och kör sedan `glom`. Git-servern tvingar personen att byta lösenord vid första inloggningen. Chatten kan inte tvinga fram ett byte, så be personen byta det själv.

Vad rollen betyder beror på boxens användarläge (beslut 29, version 1.45.0; omgjort 2026-10-25, förut efter storlek). Alla personer på en Vanlig box delar en agentmiljö, medan en Fleranvändare-box ger varje person en egen:

	Vanlig box	Fleranvändare
Antal konton	Inget tak	Inget tak (katalogen styr)
Roll `admin`	Full åtkomst	Ser byggraderna (Bygg på boxen, Claude, Grok), hanterar boxen och agentvakten
Roll `medlem`	Full åtkomst: byggraderna, och byggagenten har root på maskinen	Ser i kunskapssökningen bara `~/kunskap`, BOXEN.md och de projekt git-servern ger personen läsrätt till; byggraderna syns inte
Hemsida från chatten	Full åtkomst, som för övrigt	Bara admin, den som skapade den eller någon med skrivrätt i projektets repo

	Vanlig box	Fleranvändare
Agentmiljö	Delad; ingen agentvakt	En arbetsyta och ett Linux-konto per person; agentvakten styr nivåer och kostnad
Katalog: AD ingår, Entra ID kommer	Ingår inte	AD (LDAPS) ingår, Entra ID kommer
Plattform	Ubuntu eller macOS	Bara Ubuntu

Kort sagt: på en Vanlig box litar ni på alla ni bjuder in fullt ut. På en Fleranvändare-box följer chatten samma gräns som Mina projekt. Uppslaget mot git-servern görs av `gitratt`:

```
sudo /usr/local/lib/ai-boxen/gitratt anna@exempel.test kundregister   # skriv, las eller ingen
```

Lösenordsbyten, grupper och nycklar hanterar ni i chattens och git-serverns egna adminpaneler.

En inloggning för allt

Chatten, Mina projekt och lägessidan har knappen **Logga in med boxens konto**. Den skickar er till git-servern och tillbaka, så att ni slipper logga in flera gånger. Om inloggningen slutar fungera, till exempel efter att ni slagit på molnläget, räknar ni om den så här:

```
sudo aibox oidc
```

A6. Sidan AI-agenter (via kontrollpanelen)

Öppna agentens aktivering eller lägessidan från kontrollpanelen under **Inställningar → Agenter och modeller**, med boxens administratörskonto. Medlemmar kommer inte in. Fem felaktiga försök spärrar er adress i tio minuter.

Sidan visar läget på boxen: hur länge den varit uppe, ledigt diskutrymme, när den senast hörde av sig och antalet chattkonton. Därunder finns följande delar.

Agenterna: logga in och ut

Tabellen visar varje agent (Claude Code, Codex, Gemini, Grok, aider och Claude Code i chatten) med version, om den är inloggad, när den senast användes och vilken modell den pratar med.

En agent som inte är inloggad har knappen **Aktivera**:

Agent	Gör så här
Claude Code	Öppna länken, logga in hos Anthropic och klistra in koden ni får tillbaka
Codex	Öppna länken och skriv in engångskoden. Sidan märker själv när ni är klara
Gemini	Klistra in en nyckel från AI Studio

Agent	Gör så här
Grok	Klistra in en nyckel från xAI

Alla fyra går också att aktivera med en API-nyckel i stället för ett konto. Koden eller nyckeln skrivs bara till filer på boxen (de ägs av `ai` och kan bara läsas av det kontot). Den skickas aldrig till Self Production.

På en box före 1.59.0 går det också att lägga in nyckeln från portalen, under **Äldre box → Agenter och modeller** (agentens rad, Skicka till boxen). Då passerar nyckeln vår server tills boxen har hämtat den, normalt i mindre än fem minuter. Använd sidan på lägessidan om ni inte vill ha det fönstret.

En inloggad agent har knappen **Logga ut** (från 1.29.3). Den tar bort agentens nyckel och kontoinloggning från boxen men inget annat, och den frågar först. När ni loggar ut Claude Code stängs också fjärrstyrningen, och chattens Claude-sessioner startas om. Därefter kan någon annan logga in med sitt eget konto.

Fjärrstyrning

Med fjärrstyrningen jobbar ni vidare från Claude-appen eller claude.ai/code mot boxens filer i `/home/ai/fjarr`. Boxen gör bara utgående anrop till Anthropic, så ingen port behöver öppnas.

1. Claude Code ska vara inloggad med ett **Anthropic-konto med stöd för Claude Code och Remote Control**. En API-nyckel räcker inte, och då är knappen grå.
2. Under **Fjärrstyrning** fyller ni i **Namn i appen** och väljer **Behörighet**:
   - **Frågar före varje ändring** (`default`)
   - **Rättar filer utan att fråga** (`acceptEdits`)
3. Tryck **Starta fjärrstyrningen**. När sidan visar ansluten öppnar ni sessionen via länken eller i Claude-appen.
4. Med **Stoppa** stänger ni fjärrstyrningen. Samma session kan tas upp igen inom fyra timmar.

Tänk på att samtalet (era meddelanden, Claudes svar och vilka verktyg som kördes) lagras hos Anthropic så länge fjärrstyrningen är ansluten. Filerna och körningen stannar på boxen.

Modellservrar

Här ser ni de modellservrar boxen får prata med, om de svarar och vad de har laddat. Boxens egen motor heter `boxen`. Den står alltid först och går inte att ta bort. Under **Lägg till en modellserver** anger ni id, namn, sort (Ollama eller vLLM/OpenAI-kompatibel), adress, en modell för aider (valfritt) och en API-nyckel (valfritt). Tryck **Prova** innan ni lägger till servern. En ny server dyker upp som modeller i chatten inom en minut. Den server som är **standard** används av aider och `aibox fraga`.

Samma sak gör ni på maskinen så här:

```
sudo aibox modellserver                    # listan
sudo aibox modellserver lage               # svarar de, vilka modeller, vad är laddat
sudo aibox modellserver prova --sort ollama --url http://10.0.0.5:11434
sudo aibox modellserver lagg-till gpu1 --namn "GPU-servern" --sort ollama \
     --url http://10.0.0.5:11434 --modell gemma4:e4b
sudo aibox modellserver lagg-till vllm1 --namn "vLLM" --sort openai \
     --url http://10.0.0.6:8000 --nyckel-stdin
sudo aibox modellserver andra gpu1 --url http://10.0.0.7:11434
sudo aibox modellserver standard gpu1
sudo aibox modellserver ta-bort gpu1
sudo aibox modellserver tillamp             # skriv ut registret till chatten och aider igen
```

`--nyckel-stdin` gör att nyckeln läses från tangentbordet. Den hamnar då inte i argumentlistan, som alla på maskinen kan se.

Övriga delar på sidan

- **Mina projekt**: en länk till filerna och apparna via boxens HTTPS-länk (A7).
- **Kopian utanför huset**: läget och **återställningsnyckeln** (se A9).
- **Chatten**: vilka modeller som används, hur många samtal och när senast. Sidan läser bara samtalens metadata, aldrig innehållet.

Sidan stängs av med `AIBOX_ADMIN=av` i `/etc/ai-boxen/box.conf` följt av en körning av installern.

A7. Mina projekt (via boxens länkar)

Öppna boxens länk till **Mina projekt** och logga in med boxens konto. En kollega som bjudits in till en app loggar in med det lösenord hen valde själv. Mina projekt hette **Mina system** före 1.31.0. Tjänsterna på maskinen heter fortfarande `aibox-system…`.

Här byggs ingenting. Bygget sker i chatten, i raderna som heter **Bygg på boxen · …** (sedan 1.39.0, se A19). Byggaren är densamma och kunden väljer motor genom att välja rad. Knappen **Bygg i chatten** öppnar chatten med boxens första byggrad förvald (sedan 1.39.3; förut `cptr/projekt`, som är dold för den som inte loggat in hos Anthropic), på utifrån-adressen om molnläget har chatten ute, annars på boxens adress. Byggchatten, **Skapa system**, registermallen och förhandsvisningen från Mina system finns inte längre.

Fliken Filer

Fliken är förvald och har två delar:

- **Projekt** är `~/projekt` (`/home/ai/projekt`), en mapp per projekt. Det är samma kataloger som agenterna arbetar i.
- **Kunskap** är `~/kunskap`, dokumenten som boxens kunskapsindex läser (`aibox kunskap`).

Ni kan bläddra, ladda upp flera filer (eller dra och släppa dem), ladda ner en fil eller en hel mapp som zip, skapa mappar och ta bort.

- **Uppladdning** strömmas hela vägen till disken, högst 10 GB per fil. Boxen säger nej innan uppladdningen börjar om disken då skulle få mindre än 5 GB eller 10 % ledigt.

- **Uppladdningar går inte till git.** Inga commits görs. Det som ska versioneras checkar ni in själva, eller ber Claude göra det i chatten.
- **Borttaget** flyttas till `/var/lib/ai-boxen/papperskorg/filer-<datum>-<namn>` och gallras efter 30 dagar. Laddar ni upp en fil med samma namn som en befintlig hamnar den gamla där också. Vill ni få tillbaka något flyttar ni det på maskinen:

```
ls /var/lib/ai-boxen/papperskorg/
mv /var/lib/ai-boxen/papperskorg/filer-<datum>-<namn> ~/projekt/<projekt>/
```

- **Dolda filer** (`.git`, `.env`, `.venv` och andra punktfiler) visas inte och går inte att nå, och symboliska länkar följs aldrig.

Behörigheten är git-serverns:

Vem	Projekt	Kunskap
boxens administratör	ser och ändrar allt	läser och skriver
andra med boxens konto	ser projekt vars repo de har **läsrätt** till i git-servern; laddar upp, skapar mappar och tar bort med **skrivrätt**	läser
inbjudna till en app (eget lösenord)	ser inga projekt	läser

Ett projekt vars repo inte ligger i boxens egen git-server (eller som inte är ett git-repo alls) ser bara administratören. Detsamma gäller lösa filer direkt i `~/projekt`, att ta bort ett helt projekt och att skapa nya projekt i roten. Vill ni att en kollega ska se ett projekt sparar ni det i git-servern (`aibox spara`, A13) och ger kollegan rätt till repot där. Ändrade rättigheter i git-servern slår igenom inom en halv minut.

Filerna sköts av en egen tjänst, `aibox-system-filer`, som kör som användaren `ai` och bara får skriva i `~/projekt`, `~/kunskap` och papperskorgen. Webbtjänsten når den över en lokal socket.

```
systemctl status aibox-system aibox-system-filer aibox-system-runtime
journalctl -u aibox-system-filer -n 50
```

Fliken Appar

Här ligger de befintliga system som byggdes i Mina system. De körs på port 8092. Varje app har:

- **Öppna appen** och **Dela länk** (för appar i drift)
- **Versioner**: sätt en tidigare version i drift igen. Data behålls.
- **Säkerhetskopior**: ta, hämta och återläs. Varje app kopieras dagligen och före varje versionsbyte och återläsning. En återläsning kräver att appens namn skrivs in och tar först en kopia av aktuella data.
- **Medarbetare**: en personlig inbjudningslänk som gäller en gång i sju dagar. Ingen e-post skickas, ni lämnar länken själva. Välj mellan att läsa och ändra, eller bara läsa.
- **Ta bort**: stoppar appen och tar bort den härifrån. Koden finns kvar i git-servern.

Ändringar i en app gör ni i chatten.

Chatten och Mina projekt (1.31.1)

Chattens verktyg på boxens egna modeller är **git-servern** och **Boxens kunskap**. Det tidigare verktyget "Mina system" och dess nyckel (`/etc/ai-boxen/mina-system-chatt.nyckel`) är borttagna från 1.31.1, och tas bort från boxen vid uppdateringen. Claude och Grok i chatten (cptr) har sina egna verktyg och arbetar direkt i `~/projekt`.

A8. Uppdateringar

Boxen kan uppdateras på tre sätt. Alla tre kör samma skript, och alla tre kräver rätt till uppdateringar (se När Abonnemanget upphör nedan).

Väg	Vem	Krav
`sudo aibox uppdatera` på maskinen	ni	löpande abonnemang eller support, eller första året efter leverans
Uppdatera till X i portalen	ni	löpande abonnemang, eller första året efter leverans
Uppdatera automatiskt i portalen	ingen, det sker av sig självt	samma som ovan

På maskinen

```
aibox uppdatera kolla          # finns det något nyare? (kräver inte sudo)
sudo aibox uppdatera           # hämta och installera senaste utgåvan
sudo aibox uppdatera aterga    # kör den föregående installern igen
```

Skriptet gör så här:

1. Det frågar Self Productions utgivning vilken version som är senast. Har boxen redan den är det klart. Boxen skickar sin nyckel när den hämtar (från box 1.81.0); har boxen inte rätt till uppdateringar ändras ingenting, se nedan.
2. Det hämtar paketet och kontrollerar SHA-256-summan. Stämmer summan inte körs ingenting.
3. Det sparar den nuvarande installern som `/opt/ai-boxen/installer.forra` och kör den nya.
4. Misslyckas den nya installern körs den gamla igen, och boxen står kvar på sin tidigare version (utfallet `atergick`).

Bara en uppdatering i taget kan köras. En andra som startas medan den första pågår avvisas med `upptagen`. Innan git-servern byter version kopieras dess data till `/var/backups/ai-boxen/forgejo-fore-<version>-<tid>.tgz`.

Loggen ligger i `/var/log/ai-boxen/uppdatering.log` och kvittot i `/etc/ai-boxen/uppdatering.json`. Chatten och git-servern kan vara borta någon minut medan uppdateringen pågår.

I portalen

Under **Uppdateringar** på boxens kort står vilken version boxen kör och vilken som är senast. Har ni rätt till uppdateringar från portalen finns knappen **Uppdatera nu**. Boxen hämtar beställningen inom en minut. Så länge den inte har hämtats kan ni ångra den under Historik. Kör installationen igen och Starta

om boxen görs i kontrollpanelen (**Box och uppdateringar**), och finns också på boxens kort under **Om kontrollpanelen inte svarar** – för när kontrollpanelen är nere men boxen fortfarande hämtar kön (`installera-om`, `omstart` med `tjanst: boxen`, från 1.59.0).

Växeln **Uppdatera automatiskt** lägger beställningen åt er när boxen hör av sig efter att en ny version getts ut. Utan löpande abonnemang gör kryssrutan ingenting.

När Abonnemanget upphör

Rätten till uppdateringar finns så länge ni har ett löpande Abonnemang eller support, och första året efter leverans. Första året räknas från leveransen, och saknas leveransdatum från första gången boxen hörde av sig (`registrerad_forst`). Pausas eller avslutas boxtjänsten stänger det första året; ett löpande Abonnemang eller support ger fortsatt rätt.

Uppdateringar. Utan rätt får boxen inga nya versioner på någon väg: inte från portalen, inte automatiskt, inte från kontoret och, på boxar med AI-boxen 1.81.0 eller senare, inte med `sudo aibox uppdatera` på maskinen. Kommandot skriver "Uppdateringar ingår i Abonnemanget. Boxen kör vidare på X.Y.Z. Teckna Abonnemanget igen i portalen för att få senaste versionen.", ändrar ingenting och avslutar med kod 3. Boxen fortsätter att fungera på den version den har. Installation från en fil med `--fil` (offline) påverkas inte. Boxar äldre än 1.81.0 har inte spärren på maskinen och skickar inte sin nyckel; de hämtar som förut under en övergångstid som Self Production bestämmer. När den är slut får en sådan box bara ett vanligt hämtfel, och supporten hjälper till. En box från 1.81.0 som saknar sin nyckel får i stället "Boxen saknar sin nyckel. Kontakta supporten."

Tunneln. När Self Production slår på tunnelregeln, vilket sker senare och utan att något datum är lovat här, tas en box hos er (inte en hostad) utan rätt ur navet. Då slutar följande fungera:

- molnläget
- de publicerade adresserna (`*.box.selfproduction.se`)
- supportdörren
- kopian utanför huset

Chatten, git-servern och Mina system fungerar vidare i det lokala nätet på boxens LAN-adress. Hemringningen fortsätter, så boxen syns i portalen. `aibox tunnel` skriver "Tunneln ingår i Abonnemanget och är stängd. Boxen fungerar i ert lokala nät." och `aibox status` visar "Tunneln stängd — Abonnemanget har upphört". Hostade boxar berörs inte av tunnelregeln; de avslutas enligt villkoren 11.3 (a).

Få tillbaka det. Teckna Abonnemanget igen i portalen. Tunneln öppnas vid boxens nästa körning, inom ungefär tio minuter, och boxen kan uppdateras till den senaste versionen.

Operativsystemet

Ubuntu installerar säkerhetsuppdateringar (`-security`) automatiskt men startar **aldrig** om maskinen av sig själv. Planera omstarter själva.

A9. Säkerhetskopior

Nattens kopia

Varje natt (03:30 om inget annat ställts in) tar boxen en kopia till `/var/backups/ai-boxen`. De sju senaste sparas. Kopian innehåller:

- git-servern: repon, databas, konton och konfiguration
- chatten: konton, samtal, inställningar, uppladdade filer och vektordatabas
- kodsandlådans arbetsyta
- Claude Code i chatten: konto, arbetsytor och samtal
- `~/projekt`, med varje projekts git-historik
- apparna i Mina projekt: kod, historik, data och deras egna kopior
- namnen på modellerna (inte själva modellerna, de går att hämta igen)
- `box.conf`

Klockslaget ändrar ni i kontrollpanelen under **Säkerhetskopior** (på en box före 1.59.0 i portalen, under **Äldre box → Säkerhetskopior**).

```
sudo aibox sakerhetskopia                # ta en kopia nu
sudo aibox sakerhetskopia lista          # vilka kopior som finns, nyast först
sudo aibox sakerhetskopia /mnt/nas       # skriv kopian till en annan katalog
```

En kopia på samma disk skyddar mot misstag men inte mot att disken går sönder. Vill ni att nattens kopia hamnar någon annanstans som standard, sätter ni `AIBOX_BACKUP_MAL` i `/etc/ai-boxen/box.conf` till en monterad nätverkskatalog. Antalet sparade kopior styrs av `AIBOX_BACKUP_BEHALL`.

Återställa på samma box

```
sudo aibox sakerhetskopia lista
sudo aibox aterstall /var/backups/ai-boxen/aibox-<tid>.tar.gz
```

Återställningen frågar efter `ja` innan den börjar. Den tar först en kopia av läget som det är nu, och sedan flyttas befintliga data undan till `….gammal-<tid>`. Ingenting raderas, så en återställning från fel fil går att ångra. Det finns två flaggor:

- `--ja` hoppar över frågan.
- `--utan-kopia` hoppar över kopian av nuläget. Använd den bara om den kopian inte går att ta.

Kopian utanför huset

Om ni väljer nivån **Arboga** på boxens kort i portalen (Säkerhetskopior hos oss) skickas nattens kopia dessutom till Self Productions backupserver, genom boxens tunnel. Tunneln måste alltså vara på (se A11). Kopian krypteras på boxen innan den skickas, med en nyckel som bara finns på boxen. Self Production kan inte läsa den. Där ute sparas sju dagliga, fyra veckovisa och tolv månatliga kopior.

```
sudo aibox extern nyckel     # visa återställningsnyckeln
sudo aibox extern status     # senaste kopian, antal och eventuellt fel
```

Skriv ner återställningsnyckeln och förvara den utanför boxen. Den står också på sidan AI-agenter. Utan nyckeln går kopian inte att läsa, inte ens för Self Production. När ni tar en kopia för hand med `sudo aibox sakerhetskopia` skickas den också ut, om funktionen är på. Loggen ligger i `/var/log/ai-boxen/extern-kopia.log`.

Nivåer. Portalen visar fyra: Egen kopia (nattens kopia på boxen och kundens egna mål), Arboga (den krypterade kopian ovan), Dubbel (Arboga plus en andra ort och en återställningsövning varje kvartal) och Reserv (Dubbel plus en ersättningsbox hos oss inom fyra timmar). Egen kopia och Arboga växlar kunden själv mellan med knappen Kopia utanför huset; Dubbel och Reserv beställs genom oss. Den andra orten är inte igång än, och portalen säger då att kopian tills vidare bara ligger i Arboga. Tillvalet **arkiv i sju år** (`AIBOX_EXTERN_ARKIV`) gallrar kopian utanför huset som bokföring, en kopia per månad i sju år, i stället för tolv månader bakåt.

Egna kopiamål

Nattens kopia kan också skrivas till något kunden har själv (1.35.0): en **USB-disk**, en **filserver** (SMB eller NFS), en **SFTP-server** eller egen molnlagring (**S3** eller **Azure Blob**). Kopian krypteras på boxen med samma återställningsnyckel som kopian utanför huset. Mål läggs till och tas bort i kontrollpanelen under **Säkerhetskopior** (en äldre box: i portalen), eller på maskinen:

```
sudo aibox kopiamal lista
sudo aibox kopiamal lagg-till …      # se aibox kopiamal för formen per sort
sudo aibox kopiamal usb …            # gör en USB-disk i boxen till mål
sudo aibox kopiamal ta-bort <id>
```

- **USB-diskar** som sitter i boxen syns i portalen. Disken formateras första gången (etiketten `aibox-kopia`) och känns sedan igen. Med två diskar som byts varje vecka skrivs kopian till den som sitter i, och portalen säger till när en disk suttit i en vecka.
- **SFTP:** boxen skapar ett eget nyckelpar per mål. Den publika nyckeln visas i portalen och på lägessidan, att lägga i `authorized_keys` på servern.
- Varje mål rapporterar sitt läge i hemringningen. Kunden får mejl om ett mål inte fått en kopia på 36 timmar (USB-diskar: 8 dygn). Lösenordet till målet passerar portalen en gång och raderas när boxen hämtat det.
- Installern lägger till `cifs-utils`, `nfs-common` och `parted` om de saknas. `rpcbind`, som följer med `nfs-common`, stängs av och maskas: boxen är bara NFS-klient och monterar med `nolock`.
- **Läs tillbaka ur ett eget mål:** i kontrollpanelen, eller `sudo aibox aterstall --mal <id> [--fran <box-id>]`. En annan boxs kopia läses med den boxens nyckel, och den här boxens nyckel läggs sedan till i målet så att nattens kopia fortsätter skrivas dit.
- **Apparna startar igen efter en återställning.** Nattens kopia har en lista över projekten som var driftsatta och vilket som var publicerat, och återställningen driftsätter och publicerar dem igen.

Ny maskin efter en trasig box

1. Installera den nya boxen. Self Production lägger upp den åt er.
2. Gå till den nya boxens kort i portalen och öppna **Återställ från en tidigare box** under Säkerhetskopior hos oss.
3. Välj den gamla boxen och skriv in dess återställningsnyckel.
4. Den nya boxen hämtar den senaste kopian och lägger tillbaka git-servern, chatten, projekten och apparna i Mina projekt. Det som redan fanns på den nya boxen flyttas undan, det raderas inte.

Efter det kan den gamla boxen inte längre skicka kopior.

Står ni vid maskinen gör ni samma sak med:

```
sudo aibox aterstall --extern <gamla-boxens-box-id>
```

Kommandot frågar efter återställningsnyckeln. Gör beställningen i portalen först, för det är den som ger den nya boxen rätt att läsa den gamla boxens kopia.

A10. Brandväggen och egna regler

Installern **nollställer brandväggen (ufw) vid varje körning**, alltså också vid varje uppdatering. Regler som ni lägger direkt med `ufw allow …` försvinner därför vid nästa uppdatering.

Från 1.29.5 lägger ni egna regler i `/etc/ai-boxen/brandvagg.lokal`. Skriv en regel per rad, i samma form som efter `ufw` på kommandoraden. Rader som börjar med `#` är kommentarer.

```
# proxy för en egen sajt
allow 80/tcp comment 'minsajt: http'
allow 443/tcp comment 'minsajt: https'
```

Raderna läses in efter boxens egna regler. Bara `allow`, `deny`, `reject`, `limit` och `route` godtas. Andra rader, till exempel `disable` eller `reset`, hoppas över med en varning i installationsloggen.

Så här lägger ni in en ändring direkt, utan att vänta på nästa uppdatering:

```
sudo nano /etc/ai-boxen/brandvagg.lokal
sudo bash /opt/ai-boxen/installer/install.sh --steg 70-brandvagg
sudo ufw status numbered
```

Kör ni egna containrar med `-p` skriver Docker egna regler som går förbi ufw. Boxens tjänst `aibox-dockervakt` lägger därför samma begränsning i Dockers kedja `DOCKER-USER`: privata nät släpps in och allt annat stängs ute.

A11. Tunneln

Boxen står bakom er brandvägg och har ingen öppen port utåt. Tunneln är en utgående WireGuard-förbindelse från boxen till Self Production. Det är den som gör molnläget, publicering, supportdörren och kopian utanför huset möjliga.

- Tunneln är **på från leveransen** för boxar som installeras med AI-boxen 1.69.0 eller senare, tillsammans med molnläget (A12): kontrollpanelen nås utifrån direkt, utan att ni slår på något. Ni kan stänga av den. Boxar som installerats tidigare behåller den inställning de har.
- Tunneln går ut på UDP 51830 till `tunnel.selfproduction.se`. Stoppar er brandvägg utgående UDP kommer tunneln aldrig upp; portalen larmar då efter en halvtimme, och boxen fungerar som vanligt inne i ert nät.
- Nyckelparet skapas på boxen, och den privata nyckeln lämnar aldrig maskinen.

- Tunneln routar bara boxens eget tunnelnät. Boxens övriga trafik går som vanligt ut på er egen förbindelse.
- En brandväggsregel stänger ute vår ände av tunneln från boxens tjänster. Att tunneln finns ger alltså inte Self Production någon väg in. Det enda undantaget är de portar ni själva öppnar med molnläget, publicering eller supportdörren.

Är den av slår ni på den med **Slå på åtkomst utifrån** på boxens kort i portalen, eller i kontrollpanelen under **Åtkomst utifrån → Ställ in → Tunneln hem till oss** — tunneln och adresserna utifrån i ett — eller med knappen i Kom igång. Ni kan också slå på tunneln på maskinen:

```
sudo sed -i 's/^AIBOX_TUNNEL=.*/AIBOX_TUNNEL=på/' /etc/ai-boxen/box.conf
sudo aibox tunnel
sudo aibox tunnel visa
```

`sudo aibox tunnel ner` tar ner tunneln direkt. Står `AIBOX_TUNNEL=på` kvar i `box.conf` startar boxen den igen inom tio minuter. Vill ni stänga tunneln för gott väljer ni **Tunneln hem till oss: av** under Åtkomst utifrån i kontrollpanelen (det stänger också adresserna utifrån), eller sätter `AIBOX_TUNNEL=av` och kör `sudo aibox tunnel ner`.

Tunneln startar inte om hemringningen är avstängd, eller om brandväggen inte är aktiv. Loggen ligger i `/var/log/ai-boxen/tunnel.log`.

A12. Nåbar utifrån (`aibox molnet`)

Molnläget ger boxens egna tjänster var sin adress som fungerar var ni än är. Det behövs framför allt för en hostad box, eftersom ni inte har något eget nät som når den. Trafiken går in genom boxens tunnel, så ingen port öppnas i er brandvägg.

Tjänst	Adress
chatten	`https://chatt-<box-id>.box.selfproduction.se`
git-servern	`https://git-<box-id>.box.selfproduction.se`
sidan AI-agenter	`https://laget-<box-id>.box.selfproduction.se`
Mina projekt	`https://system-<box-id>.box.selfproduction.se`
apparna i Mina projekt	`https://appar-<box-id>.box.selfproduction.se`

Slå på molnläget i kontrollpanelen (**Åtkomst utifrån → Ställ in → Nåbar utifrån**) eller på maskinen:

```
sudo aibox molnet                 # vad som är öppet
sudo aibox molnet på              # allt: chatt git laget system appar
sudo aibox molnet på chatt git    # bara de tjänster ni anger
sudo aibox molnet av              # stäng
```

Tre saker att känna till:

- Tunneln måste vara på (A11).

- **Chatten måste ha ett konto först.** Annars blir den som först hittar adressen administratör. Kommandot vägrar slå på `chatt` eller `system` så länge chatten saknar konto. Kundens administratörskonto läggs i kön vid första hemringningen (A5); på en hostad box slås molnläget på av sig självt efter varje lyckat kontouppdrag, så snart chatten har ett konto.
- När chatten slås på stängs självregistreringen i chatten av, så att främlingar inte kan ställa sig i kö för konton.

`system` och `appar` måste slås på tillsammans. Valet står kvar efter uppdateringar. Står boxen i ert eget nät blir chatten och git-servern nåbara från internet för den som har ett lösenord, så tänk efter en gång extra innan ni slår på läget.

A13. Spara och driftsätta ett projekt

Spara i git-servern

```
aibox spara minprojekt
aibox spara --agare anna minprojekt
```

Projektet ska ligga i `~/projekt/minprojekt` och vara ett git-repo. Om repot saknas i git-servern skapas det under det första personliga kontot där, eller under det konto ni anger med `--agare`. Därefter committas och pushas projektet.

Driftfilen

Projektet ska ha en fil som heter `Driftfil` i sin rot:

```
namn=minprojekt
start=uv run app.py
port=9042
```

- `start=` är det kommando som startar tjänsten. Det krävs när appen ska köra direkt på maskinen.
- `port=` ska ligga mellan 9000 och 9099 om appen ska kunna publiceras.
- `namn=` är valfritt. Utan den används katalogens namn. Namnet får bara innehålla a–z, 0–9 och bindestreck.

Driftsätta

```
sudo aibox driftsatt minprojekt                  # enligt boxens driftsmål
sudo aibox driftsatt minprojekt --som container  # välj driftsmål själv
sudo aibox driftsatt minprojekt --stoppa
sudo aibox driftsatt --lista
```

Boxens **driftsmål** avgör var projektet kör om ni inte anger något annat. Standard är `container` (boxar från 1.78.0). Driftsmålet sätts vid installationen med `--driftsmal boxen|container|vm` (sparas som `AIBOX_DRIFTSMAL` i `box.conf`) och är inte längre kopplat till storlek eller användarläge. Med `--som` väljer ni ett annat steg för ett enskilt projekt:

Driftsmål	Så kör projektet	Plattform
`container` (standard)	med `docker compose` om projektet har en compose-fil, annars byggs dess `Dockerfile`	Ubuntu och macOS
`boxen`	som en systemd-tjänst `aibox-app-<namn>`, som användaren `ai`	bara Ubuntu
`vm`	i en egen virtuell maskin på er virtualiseringsvärd (ställs in med `sudo aibox vm`)	bara Ubuntu

På macOS finns bara `container`: `--driftsmal` med något annat avvisas av installern. (Före 2026-10-25 gav storleken driftsmålet: liten `boxen`, mellan `container`, stor `vm`. Den gamla flaggan `--storlek` finns kvar som reserv för äldre anrop och ger då samma karta.)

Ett projekt med `Dockerfile` men utan `start=` i Driftfilen körs som container även om driftsmålet är `boxen` (1.38.1). Porten kontrolleras redan vid driftsättningen: 9000–9099, och felet säger att 8080 är chatten och 3000 git-servern. Driftsättningen väntar en stund och tittar efter, så en tjänst eller container som dör direkt rapporteras som fel med loggens sista rader i stället för "kör". Står `EXPOSE 80` i Dockerfilen och `port=9000` i Driftfilen blir mappningen 9000→80.

Kör projektet i en container ska det skriva sina beständiga data under `/data` (miljövariabeln `APP_DATA` pekar dit). Katalogen är `~/projekt/<namn>/data` på boxen. Den finns kvar när containern byggs om och följer med i säkerhetskopian.

Loggen ligger i `/var/log/ai-boxen/driftsatt.log`. För en tjänst som kör på maskinen visar `journalctl -u aibox-app-<namn>` vad som hänt.

A14. Publicera en app

Med publicering får en driftsatt app en adress på internet. Varje app får sin egen:

```
https://<projekt>-<box-id>.box.selfproduction.se
```

Dessutom har boxen en **huvudadress**, `https://<box-id>.box.selfproduction.se`, som går till den första appen ni publicerar, eller till den ni valt med `--huvud`. Fram till 1.41 fanns bara huvudadressen och en app åt gången; från 1.42.0 ersätter en ny publicering inte de som redan är ute.

Trafiken går in genom tunneln, och i boxens brandvägg öppnas exakt appens port för exakt en avsändare, nämligen vår ände av tunneln.

```
sudo aibox publicera minprojekt           # publicera (lägger till)
sudo aibox publicera --visa               # vad som är publicerat just nu
sudo aibox publicera --av minprojekt      # ta bort den appens adress
sudo aibox publicera --av                 # ta bort alla adresser
sudo aibox publicera --huvud minprojekt   # appen får huvudadressen
```

Läs det här innan ni publicerar:

- **Exakt ett argument** (från 1.30.1): ett projektnamn, `--visa` ensamt, `--av` med eller utan projekt, eller `--huvud <projekt>`. Skriver ni något mer avbryts kommandot utan att något ändras. Innan 1.30.1 publicerade `publicera minprojekt --visa` appen och slog därmed ut den app som var publicerad.
- Namnet är projektets katalognamn: små bokstäver, siffror, punkt och bindestreck, högst 40 tecken. Det får **inte** vara ett av boxens egna tjänstenamn (`chatt`, `git`, `laget`, `system`, `appar`, och dessutom `www`, `api`, `nav`, `tunnel`), som ligger på samma domän.
- Tunneln måste vara på (A11).
- Appen måste vara driftsatt och lyssna på porten i `Driftfil` (9000–9099). Annars vägrar kommandot. Efter varje ändring i projektet körs `sudo aibox driftsatt <projekt>` igen så att containern byggs om; publiceringen ligger kvar.
- Adressen börjar fungera inom en minut. Ni får ett mejl med adressen, och boxen ringer hem direkt så att portalen visar den.
- Ta bort en adress påverkar inte appen: den fortsätter köra på boxen.

Tillståndet ligger i `/var/lib/ai-boxen/publicerat.d/<projekt>` (porten, en fil per app), och i de äldre filerna `publicerat` (huvudadressens port) och `publicerat.huvud` (huvudappens namn). Brandväggsreglerna för portarna läggs tillbaka vid varje körning av installern, och `aibox-dockervakt` släpper in portarna för kundens containrar. En box uppgraderad från 1.41 eller äldre, som bara har den gamla filen, behåller sin app som huvudadress under namnet `app` tills ni publicerar om den med namn.

Från portalen och chatten. I portalen: **Publicerat** på boxens kort (under Adressnamn och publicering) har en lista över boxens driftsatta projekt att **Publicera**, och per publicerad app **Ta bort** och **Gör till huvudadress** samt **Ta bort alla**. Det är samma skript, via uppdragskön (inställningsuppdraget `publicera`, utfallet `inte-driftsatt` om projektet inte svarar på sin port). Agenterna i chatten publicerar på samma sätt; terminalkommandona ovan är ett alternativ.

A15. Städa i git-servern

Agenterna skapar gärna nya repon, ett per prov eller idé. Från 1.30.0 kan de tas bort på ett säkert sätt:

```
aibox repon                              # alla repon, de som ändrades längst tillbaka först, med s
aibox repon ta-bort anna/provsida        # sparar en kopia och tar sedan bort repot
aibox repon papperskorg                  # kopiorna som finns
```

Innan ett repo tas bort sparas hela repot, med alla grenar och taggar, som en git-bundle i `/var/lib/ai-boxen/papperskorg`. Kopiorna sparas i **30 dagar** och rensas sedan bort automatiskt. Ärenden, wiki och releaser följer inte med i kopian, bara koden.

Så här får ni tillbaka ett borttaget repo:

```
git clone /var/lib/ai-boxen/papperskorg/<tid>-anna--provsida.bundle ~/projekt/provsida
aibox spara provsida
```

Agenterna har instruktion om att fråga er innan de tar bort ett repo som är i drift, eller ett repo som ni själva har skapat.

A16. Supportdörren

Supportdörren släpper in Self Productions support på port 22 genom tunneln, under en begränsad tid. Den är **stängd tills ni öppnar den**, och vi kan inte öppna den själva. Medan dörren är öppen har supporten full behörighet på maskinen, eftersom kontot `ai` har sudo.

Öppna dörren i kontrollpanelen (**Åtkomst utifrån → Ställ in → Supportdörren**), eller på maskinen:

```
sudo aibox support            # läget
sudo aibox support på         # öppen i 24 timmar
sudo aibox support på 48      # öppen i 48 timmar (högst 168)
sudo aibox support av         # stäng nu
```

Dörren stänger sig själv när tiden har gått ut, på tre sätt:

- en timer kör `support av`
- nyckeln i `~ai/.ssh/authorized_keys` har ett utgångsdatum som ssh själv respekterar
- en körning av installern stänger dörren om tiden redan har passerat

Dörren kräver att tunneln är på.

A17. Hemringningen

Boxen hör av sig till Self Production varje minut (från 1.67.1; en äldre box ungefär en gång i timmen), direkt efter ett lyckat konto- eller inställningsuppdrag, och när ett bygge börjar eller slutar (byggvakten, A19). Den skickar:

- box-id och kund-id, version, profil, operativsystem, modellnamn, vilka komponenter som är installerade och om de svarar, när säkerhetskopian togs, ledigt diskutrymme och när maskinen startades
- **konton** (från 1.40.0): antal och lista med e-post, namn, roll och tjänster. Aldrig lösenord
- **chattens modellrader** (1.40.1): id, namn och om raden är aktiv
- **driftsatta projekt** (1.41.0): projektets namn, driftsmål, om det svarar och porten ur Driftfilen
- **pågående bygge** (1.41.0): vilken rad i chatten som arbetar och hur länge. Aldrig vad som byggs
- **publicerade appar** (1.42.0): namn och port
- **om "Dela tal om användningen" är på, och i så fall tokenanvändningen** (1.42.0, A23): anrop, tokens, kontextstorlek per dag, rad i chatten och modell
- status för egna kopiamål och molnkonton (resultatet av provet, aldrig nycklarna)

Filnamn, innehåll i projekt, frågor och text från agenterna skickas inte. Mottagaren avvisar alla fält utöver de uppräknade (`extra="forbid"`): en ny box som skickar ett fält portalen inte känner får därför 422 på hela hemringningen. Portalen uppdateras först när fälten ändras.

Den senaste rapporten sparas på boxen med begränsad läsbehörighet (normalt 0640); en eventuell installationslogg ersätts där med uppgift om storlek. Administratören kan läsa det:

```
sudo aibox hemringning visa       # samma som /etc/ai-boxen/hemringning.json
sudo aibox hemringning            # skicka ett livstecken nu
```

Installationsloggen skickas bara om `AIBOX_LOGG_HEM=på` uttryckligen aktiverats. Standard är av. Lösenord och nycklar maskeras; kvittot anger att loggen skickats och dess storlek, inte loggtexten.

Stänga av hemringningen

```
sudo bash /opt/ai-boxen/installer/install.sh --utan-hemringning
```

Kommandot skriver `AIBOX_HEMRINGNING=av` i `box.conf` och kör installern. Valet står kvar vid senare uppdateringar. Boxen fungerar som vanligt lokalt, men tänk på följande:

- Boxens post finns kvar i kundportalen, men får ingen ny status. Inga nya uppdrag från portalen hämtas, till exempel uppdateringar eller tjänsteval.
- Tunneln går inte att starta, och därmed fungerar inte heller molnläget, publicering, supportdörren eller kopian utanför huset.
- Uppdateringar kräver fortfarande rätt till uppdateringar (A8). Har boxen den gör ni dem själva med `sudo aibox uppdatera`; har den inte, kör boxen vidare på sin version.

Slå på hemringningen igen med `sudo bash /opt/ai-boxen/installer/install.sh --med-hemringning`. Vill ni bara stoppa installationsloggen sätter ni `AIBOX_LOGG_HEM=av` i `box.conf`. Observera att installern (kontrollerat mot 1.42.1) inte bevarar den raden, så den måste läggas in igen efter varje uppdatering.

A18. Loggar och felsökning

Logga in som `ai` (inte root, se A2) och börja med:

```
sudo aibox status
aibox logg 100
```

Loggarna ligger i `/var/log/ai-boxen/`:

Fil	Gäller
`install.log`	installationen och varje uppdatering
`uppdatering.log`	`aibox uppdatera`
`uppdrag.log`	beställningar från portalen
`hemringning.log`	hemringningen
`tunnel.log`	tunneln
`konton.log`	kontoändringar
`modellservrar.log`	modellserverregistret
`driftsatt.log`	driftsättningar
`extern-kopia.log`	kopian utanför huset
`oidc.log`	inloggningen "boxens konto"

Fil	Gäller
`chattverktyg.log`	chattens verktyg
`post.log`	posten: id, storlek, avsändare och mapp, aldrig ämne eller innehåll

Loggar lagras på boxen. Installationsloggen kan skickas under piloten (A17), och om ni aktiverar syslog-vidarebefordran skickas valda loggrader till er loggserver (A24). För beställningar ser portalen bara ett utfallsord, till exempel `ok`, `fel` eller `atergick`.

Tjänster och containrar:

```
systemctl list-timers 'aibox-*'
systemctl status aibox-admin aibox-uppdrag.timer aibox-hemringning.timer
journalctl -u aibox-admin -n 50
sudo docker ps
sudo docker logs --tail 50 aibox-webui      # chatten
sudo docker logs --tail 50 aibox-forgejo    # git-servern
```

Vanliga problem:

Symtom	Trolig orsak	Gör så här
Inloggningen som root hänger och kopplar ner	moln-imagen spärrar root	logga in som `ai`
Chatten har inga modeller	boxen levereras utan lokal modell	`aibox modeller hamta gemma4:e4b` eller `llama3.2`, eller aktivera en agent på lägessidan
Claude i chatten svarar "Not logged in"	Claude Code är inte inloggad	aktivera Claude Code på lägessidan
En regel för port 80/443 försvann efter en uppdatering	regeln lades direkt med ufw	lägg den i `brandvagg.lokal` (A10)
`aibox status` säger att modellen kör på processorn	modellen fick inte plats på grafikkortet, eller drivrutinen saknas	se gpu-raden; står det "NVIDIA-kort utan drivrutin", starta om maskinen
Portalen säger att boxen är tyst	ingen hemringning på tre timmar	kontrollera nät och disk, och kör `sudo aibox hemringning`
Hemringning, beställningar och tunnel faller samtidigt	en trasig rad i `/etc/ai-boxen/box.conf` (känt på fysiska boxar före 1.28.4)	öppna filen, ta bort raden som inte har formen `NAMN=värde`, kör `sudo aibox uppdatera`
Disken är nästan full	gamla images eller loggar	`df -h`, `sudo docker system df`; uppdateringen till 1.29.1 och senare städar gamla images

Symtom	Trolig orsak	Gör så här
En publicerad adress ger timeout	brandväggsregeln för appens port saknas, eller appen kör inte	`sudo aibox publicera --visa`, `sudo ufw status numbered`, `sudo aibox driftsatt --lista`; från 1.39.2 lägger installern tillbaka reglerna efter varje körning, och från 1.42.1 släpps flera publicerade appar in (före det blev två portar ett tal)
Chatten visar inga Claude-rader	boxen har inget Claude-konto (medvetet från 1.39.1)	logga in Claude Code på lägessidan (A6)
En byggrad "Bygg på boxen · ..." saknas	motorn saknas: navet av, modellen inte hämtad, eller ingen inloggning	`sudo aibox modellserver lista`; raderna skapas av `byggmotorer` (A19)

Kommer ni inte vidare: öppna supportdörren (A16) och hör av er till hej@selfproduction.se, eller fråga supportchatten under **Hjälp och support** i portalen.

A19. Chatten: byggrader och hemsidor

Chattens modellväljare har fyra sorters rader, byggraderna först:

Rad	Motor	Finns när
`Bygg på boxen · qwen3-coder`	navets gx10	**Vår GPU-maskin** är påslagen
`Bygg på boxen · gemma4`	navets it-slav	**Vår GPU-maskin** är påslagen
`Bygg på boxen · <boxens egen modell>`	modellen i `AIBOX_MODELL` på boxen	modellen är hämtad (1.40.0)
`Bygg på boxen · Claude`	Claude Code	kunden är inloggad hos Anthropic
`Bygg på boxen · Grok`	Grok	Grok är aktiverad

Byggaren är en agentloop som läser och skriver filer, kör kommandon, provar, sparar i git-servern och driftsätter. Det är bara motorn som byts när kunden väljer rad. Ordet Claude står bara på raden där motorn är Claude. Den egna modellen finns för den som saknar både navet och Claude, till exempel en hostad box som är en Mac mini utan grafikkort: bygget går långsammare, men det går.

- Raderna skapas av `byggmotorer` (kör av installern, av `aibox modellserver` när en server läggs till eller tas bort, och av GPU-knappen i portalen). Varje rad är en arbetsyta `~/bygg-<motor>` med länken `projekt` till kundens projekt, och motorerna står i `/etc/ai-boxen/motorer.json`.
- **Claude-raderna** (`Bygg på boxen · Claude`, `Claude`, `Claude Opus` ...) visas bara när boxen har ett Claude-konto (1.39.1). Utan inloggning körde de annars navets lokala motor under namnet Claude. De byts in eller ut några sekunder efter in- eller utloggning hos Anthropic.
- **Förval.** På en box utan Anthropic-inloggning är den första byggraden förvald, så att det första kunden skriver går till något som kan bygga. Kundens eget val rörs inte. En ny box utan inloggning får qwen3-coder på gx10 som agentmotor.

- **Bygge pågår.** `bin/byggvakt` ser om en agent arbetar i en byggyta: en process vars CPU-tid ökat sedan förra minuten, eller som kör just nu. Uppdragskön kör den varje minut och ringer hem när ett bygge börjat eller slutat, så att portalen säger "bygge pågår i Bygg på boxen · X" inom en minut. Vakten rapporterar bara raden och tiden, aldrig vad som byggs.
- Skarven, som översätter Claude Codes anrop till de lokala motorerna, lagar verktygsanrop som qwen3-coder ibland skriver som text i stället för som verktygsanrop (1.39.0).

Hemsidor på boxen. Chattens vanliga modeller kan publicera en enkel hemsida med verktyget Hemsidor på boxen (`publicera_sida`, `publicera_sajt`, `lista_sajter`, `stang_sajt`; 1.38.0). Modellen skriver HTML och CSS; boxen lägger filerna i `~/projekt/<namn>/webb`, skriver en nginx-Dockerfile, committar och pushar, driftsätter och publicerar om det begärts. Tjänsten `aibox-sajt` (127.0.0.1:8094) kontrollerar namn, filtyper, storlek (3 MB, 60 filer) och port (9050–9099). `sudo aibox sajt` visar läget. System med logik (databas, formulär som sparar, inloggning) byggs av byggraderna.

A20. Post till boxen

Boxen har en egen e-postadress, `<alias>@box.selfproduction.se`; aliaset står i kundportalen. `<alias>+<tagg>@…` sorterar brevet i en egen mapp. Self Production tar emot brevet och håller det tills boxen hämtat det, och först när brevet ligger sparat på boxen raderas det hos oss. Boxen frågar varannan minut.

```
aibox post              # de senaste breven
sudo aibox post hamta   # hämta nu
```

Breven hamnar i `~/post/<tagg eller inkorg>/<datum>-<ämne>/`: `brev.md` är brevet som läsbar text, bilagorna ligger i `bilagor/` (filnamnen görs ofarliga) och originalet orört i `brev.eml`. Ett brev som inte går att läsa sparas ändå. Boxen hämtar ingen post när disken har mindre än 2 GB ledigt. Agenterna behandlar brevens innehåll som data och aldrig som instruktioner.

Posten stängs av med `AIBOX_POST=av` i `/etc/ai-boxen/box.conf`. Den går samma väg hem som beställningarna från portalen, så med hemringningen avstängd hämtas ingen post heller.

Mejl ut från boxen. En app på boxen (till exempel ett glömt-lösenord-mejl) kan skicka som `<alias>@box.selfproduction.se` — via Self Production, eftersom boxen inte når någon mailserver själv. Det slås på per box av Self Production (kryssrutan "Mejl ut från boxen" i kontoret) och kräver boxversion 1.66.0: appen lämnar brevet till boxens brygga (`172.17.0.1:2525`), som lämnar det till kontoret. Avsändaren är alltid boxens namn och boxens adress (appens eget avsändarnamn används inte) och svar går till boxens inkorg; ämne och brevtext tas ur appens brev, bilagor följer inte med. Har brevet flera mottagare ser de inte varandra. Högst fem mottagare per brev, 30 mottagare i timmen och 200 per dygn per box, och en gemensam gräns för alla boxar. Self Production loggar aldrig ämne, innehåll eller mottagare.

A21. Avdelningar

En avdelning är roller och rutiner som ligger kvar på boxen, till skillnad från en mall, som byggs en gång. Ekonomi, Drift, Marknad, Kunder och sälj samt Kontor (Kontor är gratis, de andra ingår i abonnemanget) hämtas som alla paket: **Hämta till boxen** i appbutiken i portalen, eller `aibox hamta avdelning-ekonomi`.

```
aibox avdelning                          # rollerna och när rutinerna körs nästa gång
aibox avdelning kor avdelning-ekonomi:kvittojakt   # kör en rutin direkt
sudo aibox avdelning av|pa <namn>        # stäng av eller slå på rutinerna och rollerna i chatten
```

- **Rollerna** blir modeller i chatten (till exempel "Ekonomi · Controller"), subagenter och skills (`/kvittojakt`) för Claude Code, och står i `AGENTS.md` för Codex och Gemini.
- **Rutinerna körs av sig själva** enligt schemat, till exempel kvittojakten vardagar 07:30. Resultatet hamnar i `~/projekt/<avdelning>/rapporter/`, committas och kommer med i kunskapsindexet. Utan aktiverad Claude, eller utan vald modellserver, skriver rutinen det i rapporten.
- **Avdelningen förbereder, människan beslutar.** Ingen roll bokför, betalar, skickar, publicerar eller ändrar i produktion själv; det som kräver ett beslut hamnar under "Behöver beslut" i rapporten. En rutin som körs utan tillsyn får läsa och skriva i sin egen katalog och läsa posten och kunskapen, men inte radera, köra sudo eller nå andra maskiner.
- `LOKALT.md` är kundens fil (attestordning, kanaler, system, egna regler). Alla roller läser den, och den skrivs aldrig över. En borttagen avdelning tar bort sina egna timrar.

A22. Molnkonton

Agenterna kan bygga och drifta miljöer i kundens eget moln. Kunden lägger in en AWS-åtkomstnyckel, en Azure-tjänsteprincip eller (version 1.45.0) en Viploy-nyckel i kontrollpanelen (**Anslutna molnkonton**), eller på maskinen:

```
sudo aibox molnkonto lista           # läget, som JSON
sudo aibox molnkonto prova aws       # svarar kontot?
sudo aibox molnkonto ta-bort aws     # glöm kontot på boxen
```

`molnkonto satt <aws|azure|viploy>` tar uppgifterna som JSON på stdin; portalen är det vanliga sättet att lägga in dem.

Viploy är enklare än molnen: bara en API-nyckel (`vibe_…`, skapad under Connect your AI → Create key på viploy.se). Boxen skriver den i `~/.viploy/config.json` och `~/.aibox/moln/viploy.env`, installerar `viploy` med Viploys eget installationsskript och provar nyckeln mot api.viploy.se. Portalen visar nyckelns fyra sista tecken och hur många projekt kontot har. BOXEN.md berättar för agenterna hur de driftsätter där: `viploy deploy <namn>` i projektkatalogen ger `https://<namn>.viploy.se`; en egen Dockerfile används inte, och gratisplanen har inget internet ut från appen. Viploy är rätt när appen ska stå ute och vara nåbar oberoende av boxen; `aibox publicera` när den ska stå på boxen, nära kundens data.

Boxen skriver uppgifterna där verktygen läser dem (`~/.aws/credentials` och `~/.aws/config` för AWS, `az login` som tjänsteprincipen för Azure, och `~/.aibox/moln/<moln>.env` för det som vill ha miljövariabler) och provar att kontot svarar. Portalen visar resultatet (kontonummer eller prenumeration, och om det svarade), aldrig nycklarna. I dagens kontrollpanel hanteras hemligheten på boxen, utan att skickas till kundportalen; den står aldrig i `/etc/ai-boxen`, loggen eller hemringningen. `aws` och `az` installeras när det första kontot läggs in, inte på varje box. `BOXEN.md` ger agenterna reglerna: säg vad det kostar innan något skapas, riv det som provats, tagga allt med `aibox=<box-id>`, håll er i Sverige och EU, infrastruktur som kod i repot.

A23. Tokenmätningen

`sudo aibox tokens` visar hur mycket agenterna använt modellerna: anrop, tokens in och ut, cachade tokens, största kontext och antal sessioner, per dag, rad i chatten och modell. `bin/tokenmatning` läser Claude Codes sessionsloggar (`~/.claude/projects/<arbetsyta>/*.jsonl`) inkrementellt; alla Bygg på boxen-rader, Claude-raderna, fjärrstyrningen och terminalen kör samma agent. Arbetsytor den inte känner igen räknas som "Annat", och Open WebUI:s vanliga chattar mäts inte. Dagsfilerna ligger i `/var/lib/ai-boxen/tokens/` i 90 dagar.

Bara tal, aldrig text, filnamn, prompter eller kod. De senaste 30 dagarna går med i hemringningen när `AIBOX_FORBATTRA` är på. Det är på som standard. Kunden stänger av i kontrollpanelen (**Agenter och modeller → Dela tal om användningen**), och en administratör kan göra det vid installationen:

```
sudo bash /opt/ai-boxen/installer/install.sh --utan-forbattring
```

Av betyder att talen stannar på boxen. Kunden ser talen i boxens kontrollpanel under Agenter och modeller; Self Production ser dem summerade över alla boxar som delar dem.

A24. Lokal driftövervakning (1.74.0)

På Linux finns tidsservrar, syslog och SNMP under **Inställningar → Åtkomst utifrån** i boxens kontrollpanel. Ange upp till fyra egna NTP-servrar. Syslog kan skickas till er loggserver med UDP, TCP eller TCP med TLS; använd provknappen för att kontrollera mottagningen. Syslog innebär att logginnehåll lämnar boxen.

SNMP är av tills ni aktiverar det. Välj helst SNMPv3 och ange tillåtna källadresser. Övervakningen läser system-, nät-, disk-, last- och minnesvärden; den ändrar inte boxen. Hemringningen rapporterar bara om NTP, syslog och SNMP är aktiverade, inte serveradresser eller lösenord. Funktionerna finns ännu inte på macOS.

A25. Sårbarhetsbevakning och provet av kopiorna (1.84.0)

Sårbarhetsbevakning

Sårbarhetsbevakning är ett tillägg som kunden tecknar per box. Varje vecka söker boxen igenom git-repona i sin egen git-server efter kända sårbarheter i beroenden (trivy) och efter lösenord och nycklar i koden (gitleaks). Utan tillägget gör boxen ingenting: portalen svarar 403 (`ej-tecknad`) på databasen och skriptet slutar tyst.

När. Linux: `aibox-kodvakt.timer`, måndagar 05:30 (upp till en halvtimme senare; en missad vecka tas igen när boxen startar). macOS: ett launchd-jobb måndagar 05:30; är Macen avstängd då hoppas veckan över.

Vad som händer (`sudo /usr/local/lib/ai-boxen/kodvakt kor`, som root):

1. Boxen hämtar sårbarhetsdatabasen från portalen (omkring 140 MB, kontrollerad mot en digest).

2. Repona kopieras ur git-servern till en katalog som bara root läser, och den senaste versionen (HEAD) av varje repo packas ut till en katalog som skannern får läsa. Kundens egna `.gitleaksignore` tas bort ur den.
3. Skanningen körs som användaren `kodvakt`, utan anslutningar ut. Linux: enheten `aibox-kodvakt-skanna.service` med `PrivateNetwork=yes`. macOS: en pf-regel som stoppar `kodvakt` tcp och udp; skanningen körs bara när regeln ligger i brandväggen, annars felet `natsparr-saknas`. Namnuppslag stoppas inte på macOS, de sköts av systemet.
4. Talen går till portalen, och rapporten skrivs till `~/kunskap/kodvakt/<datum>.md` för användaren `ai`: per projekt en tabell över sårbarheter (paket, version, rättad version, svårighet, sårbarhet, fil) och en över hemligheter med fil och rad, aldrig själva hemligheten.

Vad som går hem: antal fynd per allvarlighet (kritisk, hög, medel, låg, okänd), hur många som har en rättad version, antal hemligheter och projekt, skannrarnas versioner och databasens datum. Inga paket-, repo- eller filnamn. Portalen visar betyget under Granskning: rött vid en hemlighet, en kritisk sårbarhet med rättning eller tre höga med rättning, också när skanningen inte gick hela vägen (talen gäller då de repon som gick att skanna); gult vid en hög, medel eller okänd sårbarhet med rättning, vid ett fel och när databasen är äldre än tio dygn; annars grönt. Låga sårbarheter och fynd utan rättning syns i sammanfattningen men ändrar inte betyget.

När betyget är gult av ett fel. Ett fel ger en rad i `/var/log/ai-boxen/kodvakt.log` och raden `kodvakt` i `/var/lib/ai-boxen/ofullstandigt`, som går hem och blir larmet Installationen är inte klar tills en körning lyckas. Läs loggen; texten i portalen säger bara vilket slag av fel:

Portalen säger	Betyder	Gör så här
sårbarhetsdatabasen saknades på boxen (`db-saknas`)	boxen fick ingen databas: tunneln eller portalen svarade inte, eller tre hämtningar var redan gjorda samma dygn	kontrollera tunneln (A11) och kör `sudo /usr/local/lib/ai-boxen/kodvakt kor` igen; hjälper det inte, hör av er till oss
ett repo gick inte att hämta eller skannern gav ett fel (`skanner-fel`)	ett eller flera repon hoppades över, eller en skanner föll; de övriga skannades	läs `kodvakt.log`
nätspärren på boxen saknades (`natsparr-saknas`, macOS)	pf-regeln för `kodvakt` låg inte i ankaret	`sudo /usr/local/lib/ai-boxen/pf-ladda`, sedan `pf-ladda --kontrollera-kodvakt`
Sårbarhetsdatabasen på boxen är från	databasen är äldre än tio dygn	boxen har inte kunnat hämta en ny; kontrollera tunneln (A11), kör `kodvakt kor` och hör av er till oss om det inte ändras

Begränsningar.

- Bara den senaste versionen av koden skannas, inte äldre commits. En hemlighet som ligger kvar i historiken hittas inte, och att ta bort raden räcker inte: nyckeln ska bytas.
- trivy söker beroenden som står i projektens beroende- och låsfiler. Java-arkiv (JAR) skannas inte, och den kod kunden själv skrivit analyseras inte (inga kodmönsterregler).
- gitleaks kör sina standardregler. Kundens egen `.gitleaks.toml` och `.gitleaksignore`, och `gitleaks:allow` i koden, tystar ingenting.

- trivy och gitleaks hämtas vid installationen (steg 72), pinnade och kontrollerade mot en kontrollsumma i `versioner.env`. Går hämtningen eller summan fel installeras ingenting, och raden `kodvakt` står i `ofullstandigt` tills nästa körning av installationen. Grundbox-ISO:n tar inte med skannrarna.

Provet av kopiorna

En kopia som aldrig lästs tillbaka är en förhoppning. Från 1.84.0 provar boxen själv, ungefär en gång i månaden, att kopiorna går att läsa tillbaka:

- **Den egna kopian.** Senaste kopian i `/var/backups/ai-boxen` läses igenom, databaserna kontrolleras (`PRAGMA integrity_check`) och git-repona (`git fsck`). Provet packas upp i en katalog bredvid kopian (`.prov-<tid>`) och tas bort igen. Kopian rörs inte. Finns inte dubbelt så mycket ledigt utrymme som provet behöver blir utfallet `utrymme` och ingenting packas upp.
- **Kopian i Arboga** (om den är på). Senaste kopian läses tillbaka ur kopian utanför huset till samma ställe och kontrolleras på samma sätt, och månadens tolftedel av repot läses igenom (`restic check --read-data-subset=<månad>/12`). Varje block i repot har alltså lästs en gång om året bara om provet görs varje månad och läser hela kopian. Kopian och repot ändras inte. Är kopian så stor att hela inte hinner läsas på cirka 100 minuter med 4 MiB/s provas en del i stället (`omfang: del`): början av arkivet (256 MB) och ett slumpat urval av repot läses, databaserna och git-repona kontrolleras inte, och månadens tolftedel läses inte. Provet avbryts efter 110 minuter och räknas som fel.

Timern (`aibox-kopieprov.timer`, 04:40, upp till 20 minuter senare; på macOS ett launchd-jobb 04:40) frågar varje natt om det är dags. Provet görs var 28:e dygn på boxens egen dag (räknad ur box-id:t, så att inte alla boxar provar samma natt), och senast när 35 dygn gått. Ett prov som föll görs om nästa natt; efter tre fel i rad en gång i veckan. En ny box utan någon kopia än provar ingenting.

```
sudo aibox sakerhetskopia prova      # provar båda nu; sista raden är ok, fel eller utrymme
```

Utfallet ligger i `/var/lib/ai-boxen/prov/senaste-lokal.json` och `senaste-extern.json` (tid, utfall, sekunder, antal filer, och för Arboga-provet `omfang`: `hela` eller `del`), går hem med hemringningen och visas i portalen under Kopior som senast provad. Loggen för Arboga-provet är `/var/log/ai-boxen/extern-kopia.log`.

Det hemringningen skickar sedan 1.84.0

Utöver det som står i A17 skickar boxen från 1.84.0 underlaget för Compliance-rapporten. Det är bara tal, ja/nej och datum:

- väntande uppdateringar och hur många av dem som är säkerhetsrättelser, om en omstart krävs, om uppdateringarna installeras automatiskt och när det senast skedde
- numren på de portar som lyssnar utanför boxen
- om SSH är på, och om lösenord och root får logga in
- om systemloggen sparas, hur stor den är och hur långt bakåt den räcker, och antal sudo-rader de senaste 30 dygnen (inget av loggmåtten på macOS)
- om disken är krypterad
- när kopiorna senast provades, med utfall, tid och antal filer, och för Arboga-provet om hela kopian eller en del provades (ovan)

Aldrig paketnamn, processnamn, sökvägar eller användarnamn. Mottagaren avvisar allt utöver dessa fält, och en ny box mot en äldre portal tar då bort fälten ur livstecknet i stället för att bli tyst.