SIbEL

CENTRAL hub

BRUGSANVISNING

ANNE One Admin

support.sibelhealth.com

IFU P/N 443-00006-DA-A

Indholdsfortegnelse

Afsnit 1. Vigtig sikkerhedsinformation

1.1 Oversigt

Dette dokument er beregnet til kvalificeret teknisk personale, der er ansvarligt for installation, konfiguration, vedligeholdelse og service af ANNE One-systemet fra Admin Hub og dets netværksforbundne komponenter. Den beskriver ikke klinisk brug eller patientvendt drift.

Tilladte serviceaktiviteter omfatter:

- Installation og konfiguration af systemsoftwaren og den understøttende infrastruktur som beskrevet i denne brugsanvisning og tilhørende installationsmanualer, SDD-SW-031-007 Central Monitoring System Installationsmanual.
- Systemovervågning, loggennemgang, backup, gendannelse, programrettelser og nedlukningsaktiviteter, der er eksplicit beskrevet i dette dokument.
- Netværks-, server- og adgangskontrolkonfiguration i overensstemmelse med de givne anbefalinger.

Forbudte handlinger omfatter:

- Ændring af software, firmware, systemarkitektur, sikkerhedskontroller eller konfigurationer uden for dokumenterede procedurer.
- Brug af udokumenterede grænseflader, legitimationsoplysninger eller bagdørsadgangsmekanismer.
- Serviceaktiviteter, der kan ændre klinisk funktionalitet, dataintegritet eller overholdelse af lovgivningen.

Producentens godkendelse kræves:

- Enhver afvigelse fra dokumenterede installations-, opgraderings-, patch-, gendannelses- eller cybersikkerhedsprocedurer.
- Manuel indgriben på database-, container- eller operativsystemniveau, der ikke er eksplicit beskrevet i denne brugsanvisning eller producentleveret servicedokumentation.

1.2 Ordliste

Tabel 1: Ordliste

Forkortelser	Definition
Brugsanvisning	Brugsanvisning
RBAC	Rollebaseret adgangskontrol
ADT	Indlæggelse-udskrivelse-overførsel
PM	ANNE View
BLE	Bluetooth lavenergi
Slutdato	Slutdato

NFC	Nærfeltskommunikation
LED	Lysdiode
IP	Indtrængningsbeskyttelse
IT	Informationsteknologi
VM	Virtuel maskine
TPM	Pålidelige platformmoduler

1.3 Symboler

Tabel 2: Symboler

Symbol	Titel	Beskrivelse
Rx ONLY	Kun til brug på recept	Føderal lov begrænser denne enhed til salg af eller efter ordre fra en autoriseret sundhedsperson.
	Se brugsanvisningen/hæfte	For at angive, at brugsanvisningen/hæftet skal læses
	eIFU	Angiver behovet for, at brugeren konsulterer brugsanvisningen eller den elektroniske brugsanvisning.
QTY	Symbol for mængde	Angiver antallet af enheder eller stykker i pakken.
EC REP	Autoriseret repræsentant i Den Europæiske Union	Angiver den bemyndigede repræsentant i Den Europæiske Union.
CE 2460	CE-mærkning	Angiver, at et produkt er blevet vurderet af producenten og anset til at opfylde EU's sikkerheds, sundheds og miljøbeskyttelseskrav. Det er påkrævet for produkter, der er fremstillet overalt i verden, og som derefter markedsføres i EU.

1.4 Producentoplysninger

- Kontakt din kundesupportrepræsentant, hvis du har et af de følgende problemer:
    - Hjælp til opsætning, brug eller vedligeholdelse af det centrale overvågningssystem
    - Sådan rapporterer du uventede handlinger eller hændelser

Sibel Health Inc.
Adresse: 2017 N Mendell St. Unit 2SE, Chicago IL 60614, USA
Telefon: (224) 251-8859
Website: www.sibelhealth.com

MDSS GmbH
Schiffgraben 41, Hannover 30175
Tyskland

Afsnit 2. Produktspecifikationer

2.1 Produktspecifikationer

Tabel 3: Specifikationer for det centrale overvågningssystem

	Centralt overvågningssystem (server)
CPU	1 × 4-kernet CPU @ 2,4 GHz
RAM	6GB
Harddiskkapacitet	OS-disk - 100 GB Datadisk - 300 GB SSD
Ekstern lagring	Ingen
Netværk	100/1000 Mbps Ethernet
Anden hardware	Uafbrudt strømforsyning
Operativsystem	Ubuntu 24.04 Noble Numbat
Understøttende software	Ingen

Tabel 4: Specifikationer for USB-drev til det centrale overvågningssystem

Udfør	iStorage
Modelnummer	IS-FL-DA3C-256-32
Lagerkapacitet	32GB
Grænseflade	USB Type C med Type-A-adapter
Dataoverførselshastighed	Læse: 310MB/s Skrive: 246MB/s
Dimensioner (mm)	Højde: 80,10 mm Bredde: 20,25 mm Dybde: 10,70 mm
Vægt	25g
Operativsystemkompatibilitet	MS Windows, macOS, Linux, Chrome, Android, tynde klienter, nulklienter, indlejrede systemer, Citrix og VMware
Krypteringsnøgler	256-bit hardwarekryptering

2.2 Sikkerhedsanbefalinger

- Sørg for at aktivere diskkrypteringen for operativsystemdisken for at understøtte datasikkerhed.
- Brug TPM eller sikker opstart før installationen.
- Brug antivirus- eller anti-malware værktøjer på værterne inden installationen.
- Kommunikation mellem tredjepartsapplikationer og komponenten i det centrale overvågningssystem kan kun udføres, hvis tredjepartsapplikationens kilde-IP er hvidlistet.
- Det centrale overvågningssystem bruger ikke et master nøglelager for at undgå risikoen for brute force, usikker lagring og sidekanalangreb.
- Regelmæssig overvågning og sikkerhedskopiering af data anbefales.
- Brug begrænsninger for brugen af fysiske eller bærbare enheder på det centrale overvågningssystems server samt det Windows-system, der skal bruges til overvågning.

2.3 Netværksanbefalinger

- Sørg for, at både PMS og det centrale overvågningssystem er forbundet til det samme lokale netværk (LAN) eller VLAN.
- Konfigurer firewalls til at netværksdæmpe brugere, der opdages med ondsindede hensigter. Begrænsning af brugerne til 10 megabits/sekund og underretter IT-administratorer om ondsindede aktører.

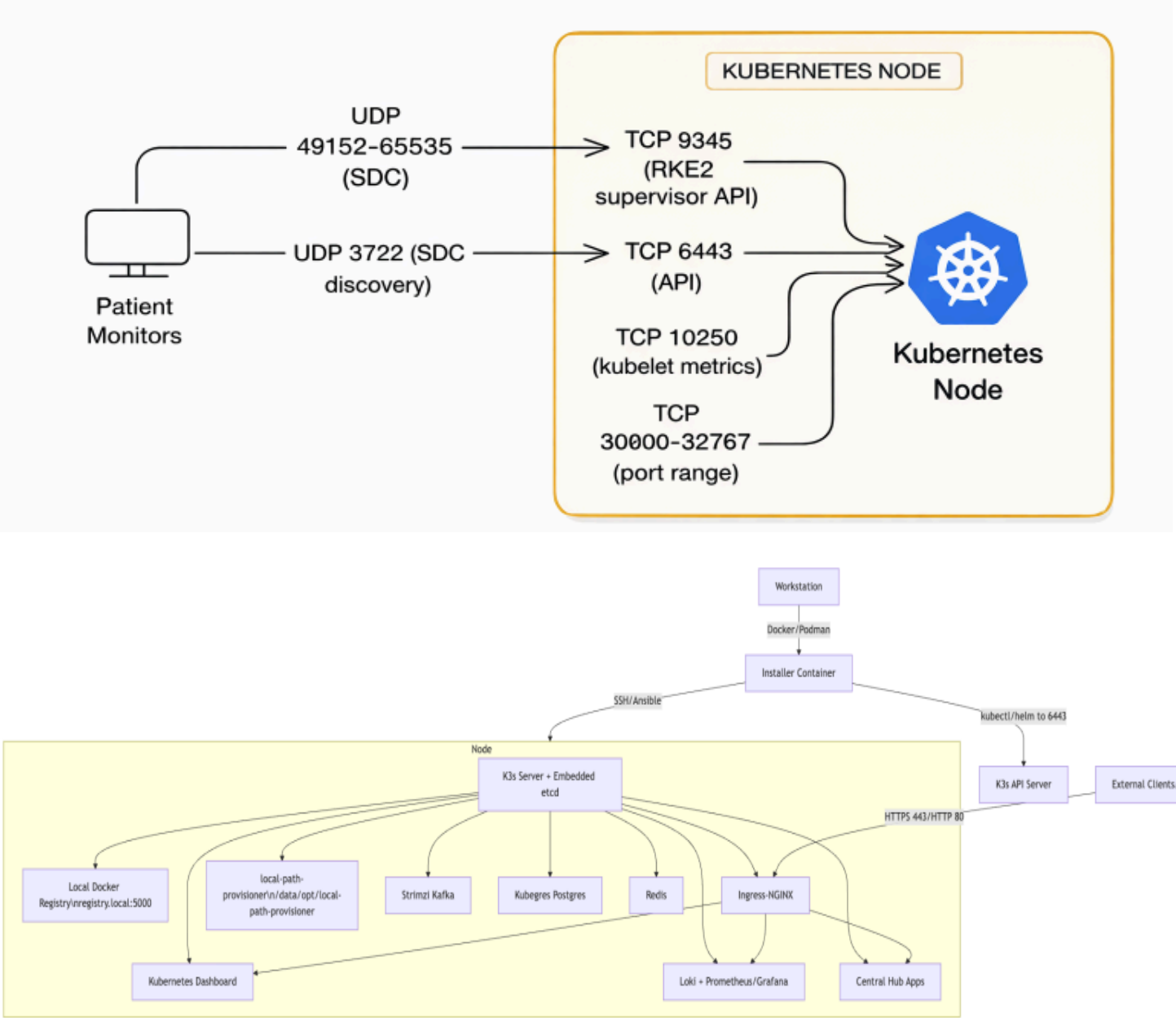
2.3.1 Konfiguration af netværksport

Det centrale overvågningssystem har den følgende portkonfiguration. Bemærk venligst, at alle ubenyttede porte skal deaktiveres.

Tabel 5: Liste Konfiguration af netværksport og beskrivelse

Port	Kilde	Destination	Beskrivelse
53	Alle Kubernetes-noder	kube-dns / CoreDNS	DNS-opløsning
80	Forskellige tjenester	auth, central-monitoring, fleet-manger, kube-prometheus-stack-grafana	HTTP-tjenester
443	Forskellige tjenester	Kubernetes-systempanel, Kubernetes API, måling-server, kube-prometheus-stack-operatør	HTTPS/API adgang
8080	Interne tjenester	hmdm-headwind-mdm, kube-prometheus-stack-alertmanager, kube-prometheus-stack-kube-state-metrics, kube-prometheus-stack-prometheus	Interne tjenesteslutpunkter
31000	MQTT-klient	hmdm-headwind-mdm	MQTT-kommunikation
5432	App-tjenester	postgres	Databaseadgang
6379	App-tjenester	redis	Redis-kommunikation

Port	Kilde	Destination	Beskrivelse
8443	Metrics scraper	kubegres-controller-manager-metrics-service	Målinger endepunkt
9090	Overvågningsværktøjer	kube-prometheus-stack-prometheus, prometheus-drevet	Prometheus UI/API
9093	Alertmanager	alertmanager-drevet, kube-prometheus-stack-alertmanager	Alertmanager API
9094	Alertmanager	alertmanager-drevet, kube-prometheus-stack-grafana-headless	Klynge beskeder (TCP)
9094	Alertmanager	alarmmanager-drevet	Klynge beskeder (UDP)
9100	Overvågningsagenter	kube-prometheus-stack-prometheus-node-exporter	Node målinger
9153	DNS metrics	kube-dns, kube-prometheus-stack-coredns	CoreDNS målinger
10250	Kubernetes-komponenter	kube-prometheus-stack-kubelet	Kubelet sikker port
10255	Kubernetes-komponenter	kube-prometheus-stack-kubelet	Kubelet skrivebeskyttet port
4194	Målingsagent	kube-prometheus-stack-kubelet	cAdvisor målinger
7946	Loki-tjenester	loki-medlemsliste	Klynge medlemskab kommunikation
3100	Logningstjenester	loki, loki-headless	Loki-logfiler
30080	Traefik	traefik NodePort (HTTP)	HTTP NodePort til indtrængen
30443	Traefik	traefik NodePort (HTTPS)	HTTPS NodePort til indtrængen



Figur 1: Diagram over centralt overvågningssystem klyngenetværk

Afsnit 3. Administrator betjeningspaneler og -tjenester

3.1 Kubernetes-kontrolpanel

3.1.1 Adgang til Kubernetes kontrolpanel

Kubernetes-kontrolpanelet er tilgængeligt via linket `https://dash.${dit-domænenavn}`.

For at kunne få adgang til kontrolpanelet skal du sørge for, at DNS-posten findes for dette domæne hos din DNS-udbyder.

Godkendelse til kontrolpanelet kan udføres ved hjælp af `kubeconfig`-fil genereret under installationen ELLER ved hjælp af et token.

Se "Generelle oplysninger om implementering af det centrale overvågningssystem" for at få oplysninger om, hvordan du får `kubeconfig`-filen.

Tokenet kan hentes fra K8S-klyngen ved hjælp af kubectl-værktøjet som følger:

Følg disse trin for at få adgang til kontrolpanel-tokenet:

1. Find filen med navnet `kontrolpanel-token.txt`, når installationsprocessen er fuldført.
2. Denne fil kan findes i `creds-` mappen i installationsbilledet.
3. Alle legitimationsoplysninger, inklusive `kontrolpanel-token.txt`, gemmes i denne `creds-` mappe.

3.1.2 Brug af Kubernetes kontrolpanel

Det centrale overvågningssystem inkorporerer et Kubernetes (K8s)-kontrolpanel for at forbedre synligheden og administrationen af det containeriserede centrale overvågningssystem. Dette værktøj er en integreret del af at opretholde den operationelle tilstand og overholdelse af kliniske systemer, og det giver kritisk indsigt og kontrol over den infrastruktur, der understøtter driften.

Nøglefunktioner og tilpasning:

- **Klyngestyring i realtid**: K8s kontrolpanel giver et realtidsoverblik over klyngetilstand, herunder nodestatus, ressourceudnyttelse og ydeevnen af implementerede applikationer. Det gør det muligt for administratorer at overvåge og administrere de Kubernetes-klynger, der er vært for Central Monitoring System-systemet, effektivt.
- **Arbejdsbyrdehåndtering**: Administratorer kan se, administrere og foretage fejlfinding af arbejdsbelastninger, herunder implementeringer, replikasæt og pods. Denne funktionalitet er afgørende for at sikre, at kliniske applikationer kører problemfrit og opfylder de ydeevnekrav, der er nødvendige for sikker og effektiv patientpleje.
- **Overvågning af navneområde**: Kontrolpanelet giver mulighed for overvågning af forskellige navneområder og tilbyder en segmenteret visning af klyngen, der kan skræddersys til specifikke kliniske applikationer eller afdelinger inden for sundhedsfaciliteterne.
- **Overvågning af ressourceudnyttelse**: Detaljerede målinger af CPU-, hukommelses- og lagerforbrug er tilgængelige, hvilket muliggør proaktiv styring af ressourcer for at forhindre ydeevneforringelse, der kan påvirke den kliniske drift.

3.1.3 Funktioner for hospitalets IT-administratorer

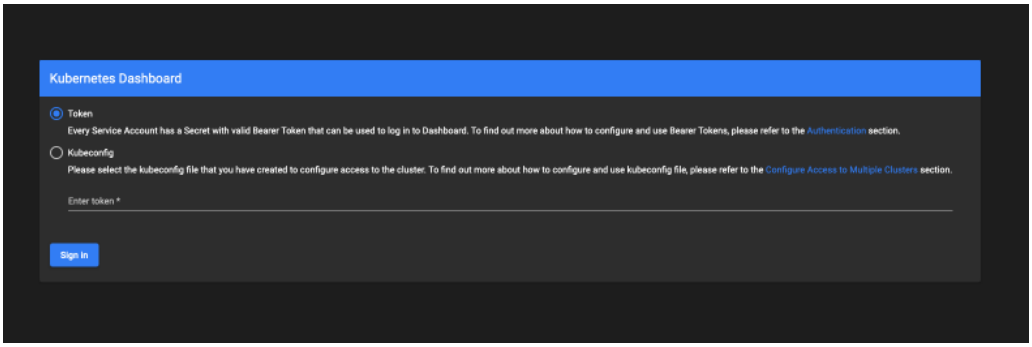
Hospitalets IT-administratorer har beføjelse til at:

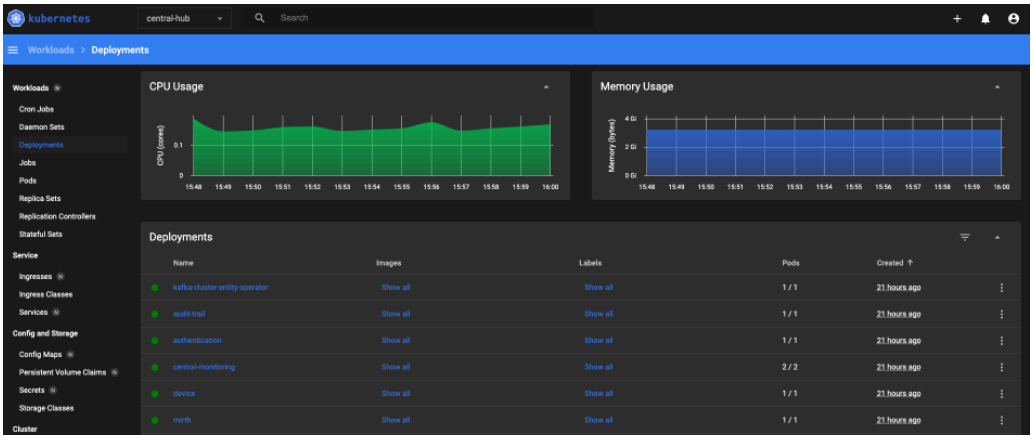
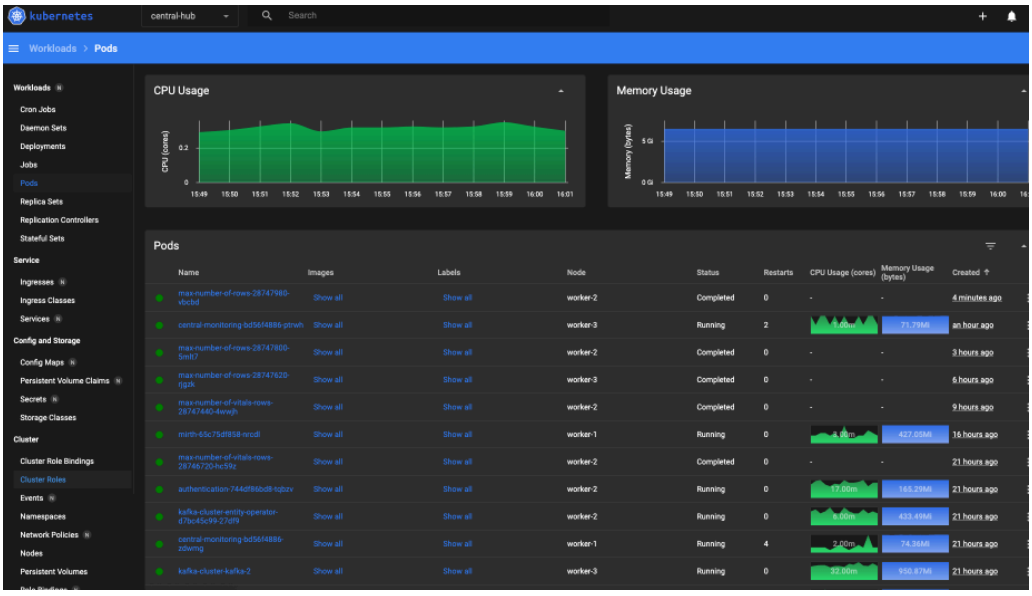
- **Implementer og administrer applikationer**: Kontrolpanelet forenkler implementeringen og administrationen af applikationer i Kubernetes-miljøet. Administratorer kan opdatere eksisterende tjenester og administrere konfigurationer direkte via :kontrolpanelet.
- **Overvåg klynge hændelser**: kontrolpanelet indeholder en omfattende log over Central Monitoring System-tjenester, hvilket giver administratorer mulighed for at spore ændringer, eksportere logfiler og hurtigt diagnosticere problemer. Dette er afgørende for at opretholde overholdelse og sikre, at eventuelle problemer, der påvirker det centrale overvågningssystems applikationer, straks håndteres.
- **Ressourcekvotestyring**: Administratorer kan indstille og håndhæve ressourcekvoter (skala) og dermed sikre, at ingen enkelt applikation eller bruger forbruger for mange ressourcer, hvilket kan kompromittere ydeevnen af andre kritiske kliniske applikationer.

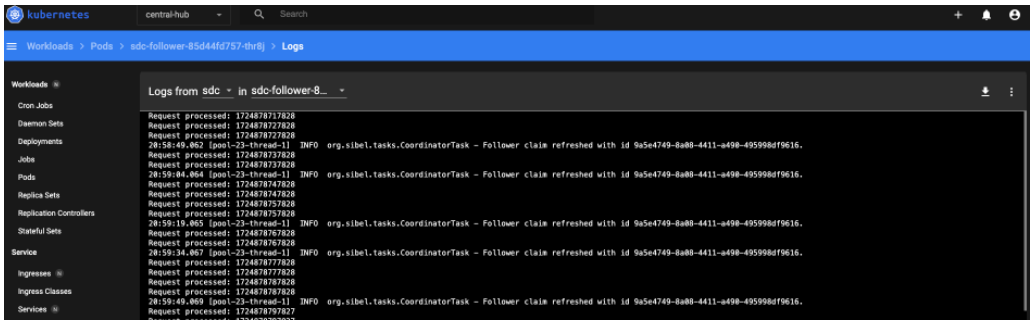
3.1.4 Overvågningsmålinger

- **Pods- og beholderovervågning**: Løbende sporing af pod-status og containertilstand for at sikre, at alle komponenter i kliniske applikationer fungerer korrekt.
- **Nodetilstand og ydeevne**: Realtidsovervågning af nodetilstand, inklusive CPU og hukommelse, sikrer, at infrastrukturen, der understøtter kliniske applikationer, forbliver robust og pålidelig.

Tabel 6: Kubernetes-overvågningsmålinger

K8s Betjeningspanel	**Billede**
Login	

Status for arbejdsbyrde	
Implementeringer	
Løbende pods	

Servicelogs	

3.2 Grafana kontrolpanel

3.2.1 Adgang til Grafana-kontrolpanel

Grafana-kontrolpanelet er tilgængeligt via linket `https://mon.${dit-domænenavn}`.

For at kunne få adgang til kontrolpanelet skal du sørge for, at DNS-posten findes for dette domæne hos din DNS-udbyder. Vi anbefaler at bruge domæne med regex, så du ikke behøver at tilføje et specifikt domæne i din DNS-udbyder (f.eks. *.{dit-domænenavn})

Følg disse trin for at få adgang til kontrolpanel-tokenet:

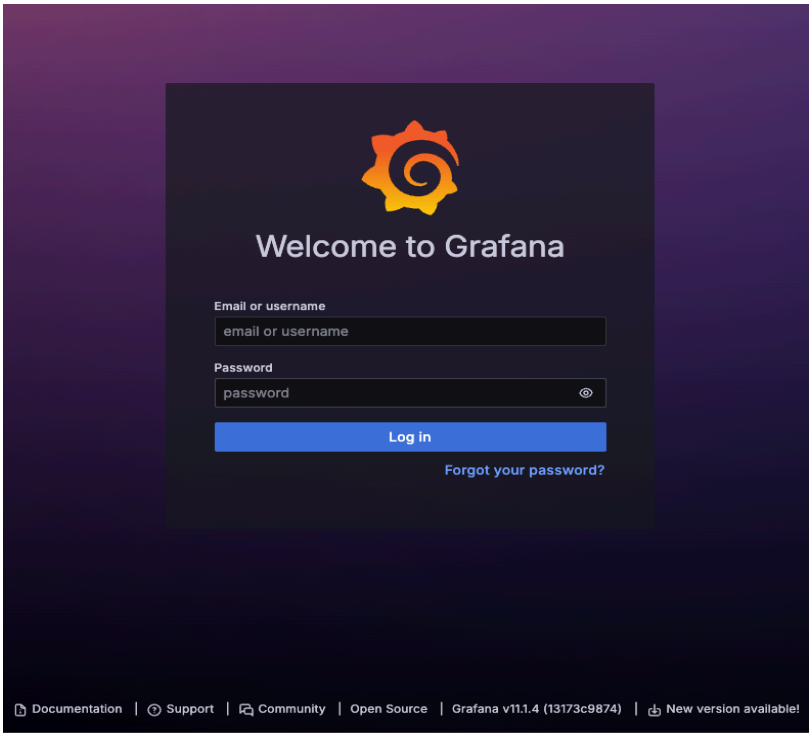
1. Find filen med navnet `monitoring.txt`, når installationsprocessen er fuldført.
2. Denne fil kan findes i creds-mappen i installationsbilledet.
3. Alle legitimationsoplysninger, inklusive `monitoring.txt`, gemmes i denne `creds-` mappe.

3.2.2 Brug af Grafana-kontrolpanel

Det centrale overvågningssystem til kliniske løsninger integrerer avancerede funktioner til hændelsesdetektion, logging, alarmering og overvågning, som er afgørende for at sikre pålideligheden og sikkerheden i kliniske operationer, herunder netværksanomalier, loginforsøg eller ændringer i systemkonfigurationen. Disse funktioner aktiveres via GPL-stakken - Grafana, Prometheus og Loki. Dette overvågningsværktøjssæt giver omfattende visualisering via diagrammer, grafer og detaljeret loganalyse, der dækker alle komponenter i det centrale overvågningssystem, herunder tjenester i det centrale overvågningssystem, infrastrukturtjenester, servertrafik og netværksovervågning.

Nøglefunktioner og tilpasning:

- **Foruddefinerede kontrolpaneler og tilpasning**: Som standard er systemet udstyret med 20+ foruddefinerede kontrolpaneler, der er organiseret af Sibel-teamet. Disse kontrolpaneler giver omfattende indsigt i forskellige driftsparametre. Derudover understøtter overvågningsplatformen fuld tilpasning af et kontrolpanel og alarmregler for at imødekomme specifikke kliniske behov.
- **Logopbevaring**: For at optimere lagring og ydeevne er standardopbevaringsperioden for logfiler indstillet til 7 dage. Denne periode er udformet under hensyntagen til balancen mellem lagerkapacitet og behovet for historiske data i kliniske miljøer.
- **Login**



Figur 2: Versionen af Grafana skal verificeres fra loginvinduet

3.2.2.1 Kompetencer for IT-administratorer

IT-administratorer har beføjelse til at:

- **Oprette brugerdefinerede kontrolpaneler og advarsler**: Administratorer kan designe et kontrolpanel, der er skræddersyet til deres operationelle behov, og oprette brugerdefinerede advarsler for at sikre proaktiv overvågning.
- **Brugeradministration**: Systemet understøtter rollebaseret adgangskontrol (RBAC), der giver administratorer mulighed for at oprette og administrere brugere med passende adgangsniveauer, hvilket sikrer en tryg og kompatibel drift.

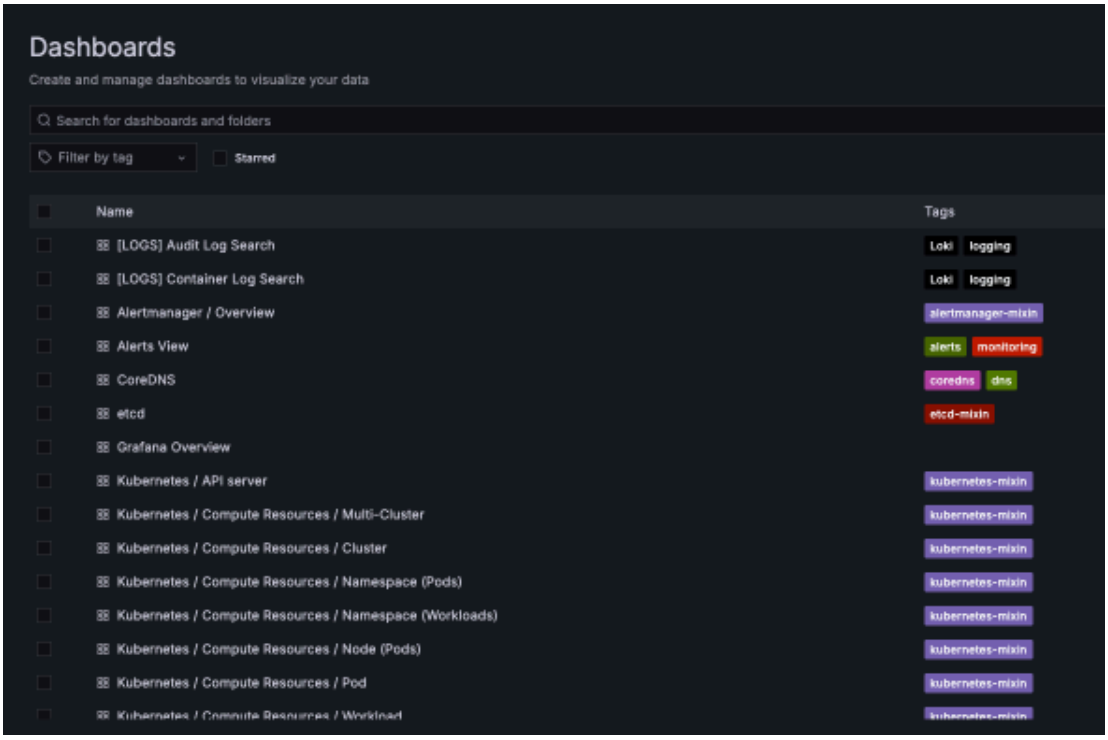
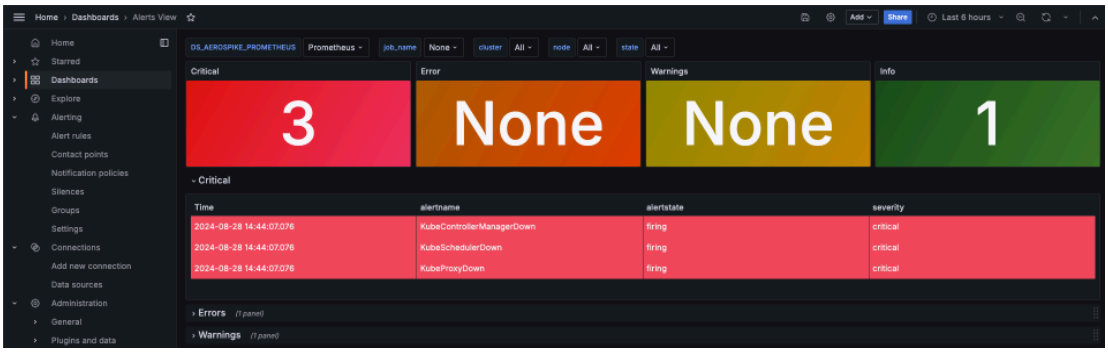
3.2.2.2 Overvågningsmålinger

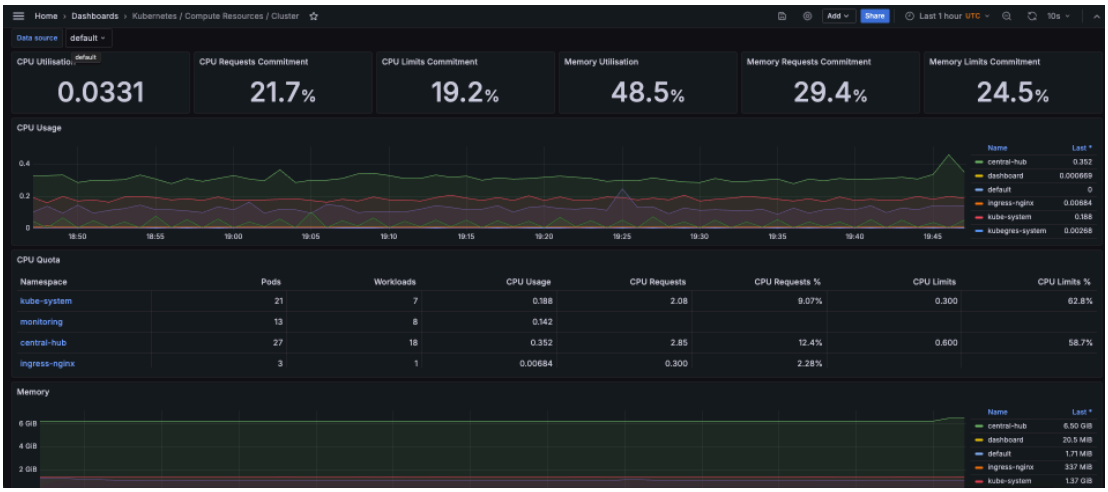
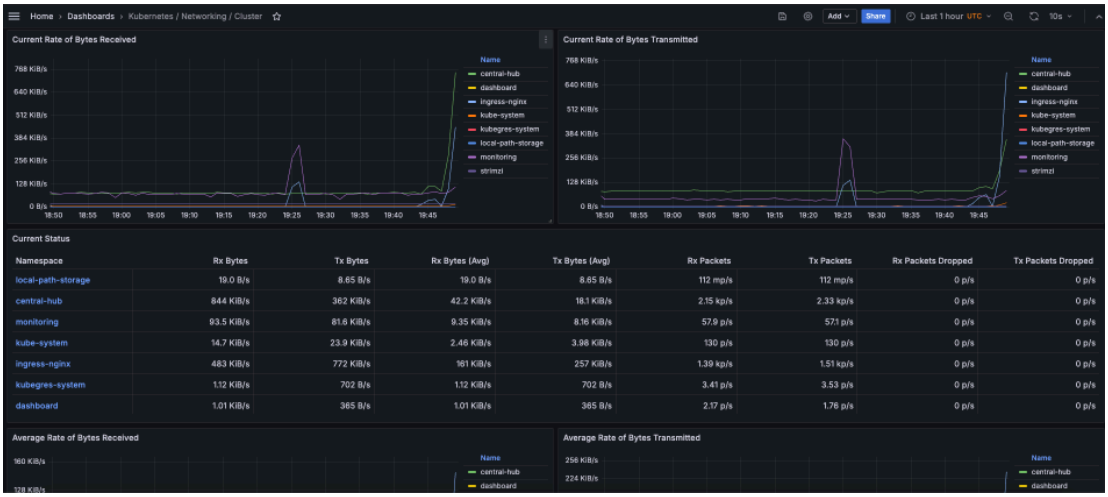
Overvågningsværktøjet tilbyder detaljerede målinger og logfiler, herunder:

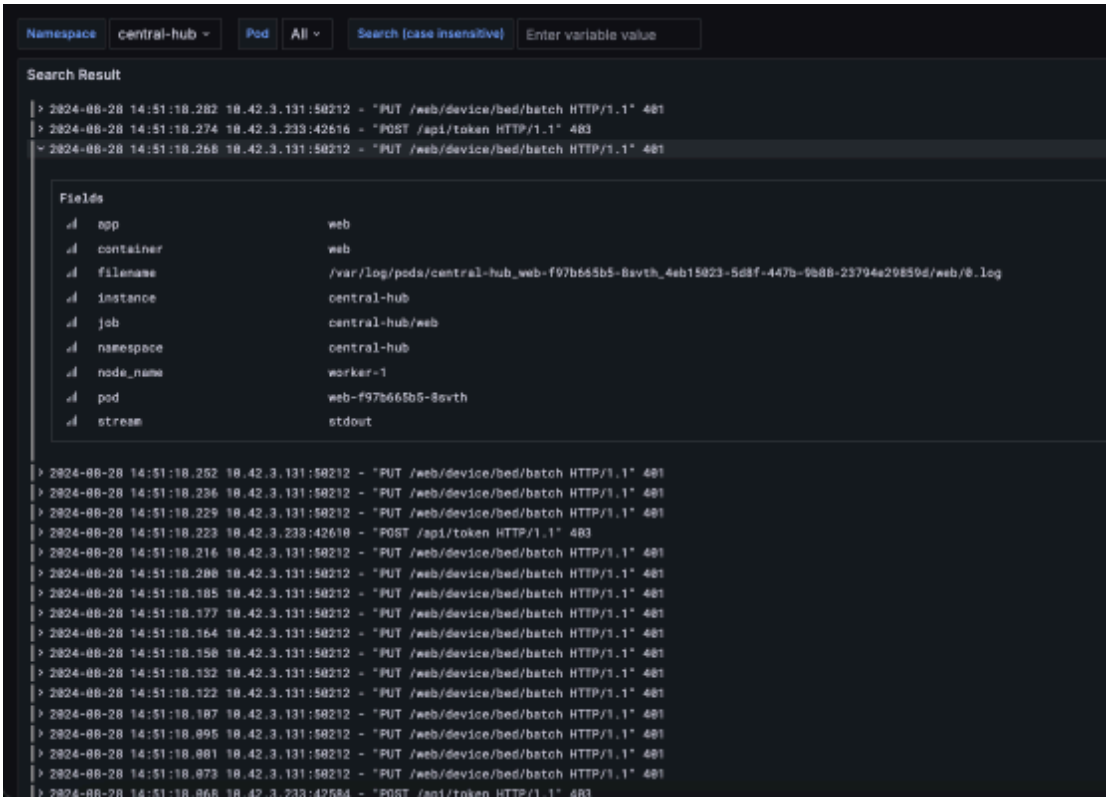
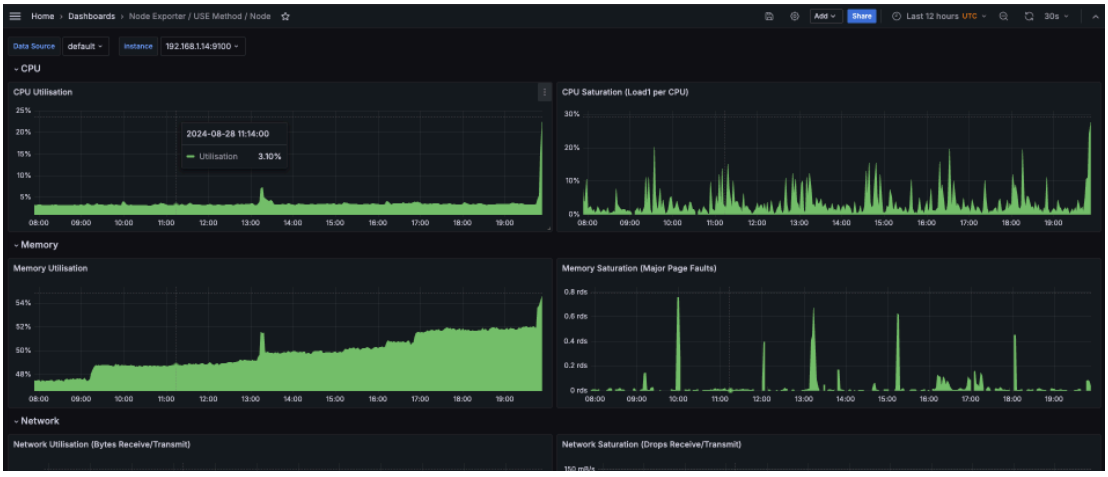
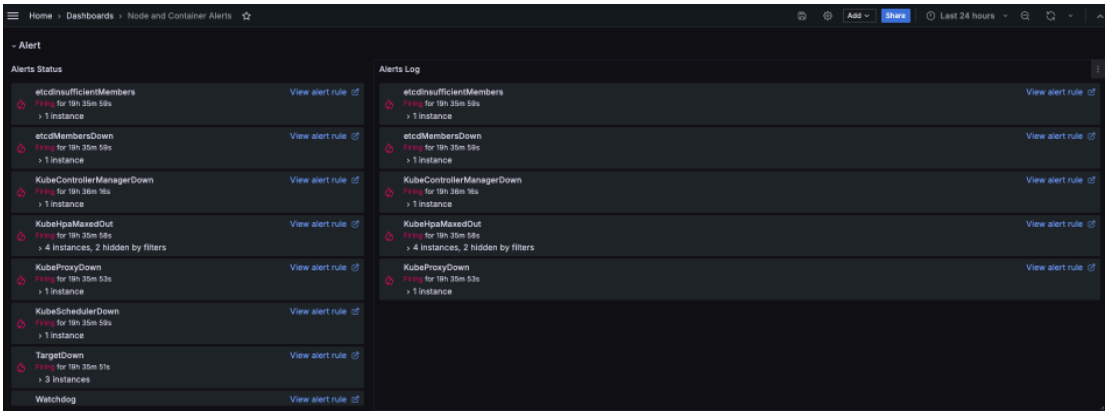
- **Statistik over servertilgængelighed**: Løbende sporing af serverens oppetid og tilgængelighed for at sikre systemets pålidelighed.
- Søgning i containerlogfiler: Effektive søgefunktioner i containerlogfiler til hurtig fejlfinding og analyse.
- **Overvågning af ressourceudnyttelse**g: Realtidsovervågning af CPU-, hukommelses- og diskforbrug på tværs af systemet.
- **Klynge- og nodeovervågning**: Omfattende indsigt i klyngeressourcer, nodeydelse og overordnet systemsundhed.
- **Overvågning af netværksarbejdsbelastning**: Detaljeret overvågning af netværkstrafik for at forhindre flaskehalse og sikre en optimal ydeevne.
- **Revisions- og proxylogfiler**: Vedligeholdelse af detaljerede revisionsspor og proxy-logfiler for at understøtte overholdelse af kliniske og lovgivningsmæssige standarder.

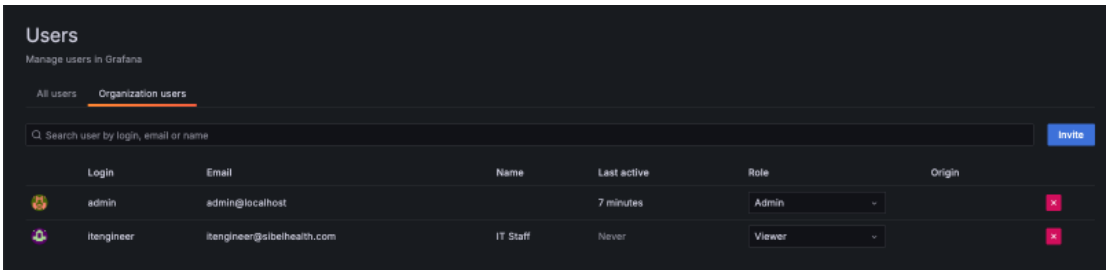
- **Logforbrugerintegration**: Systemet integreres med kompatibelt indtrængningsdetektionssystem (IDS) eller Sikkerhedsinformation og hændelsesstyring (SIEM)-løsninger.

Tabel 7: Grafana-overvågningsmålinger

Grafana	Billede
Kontrolpanel	
Advarselsvisning	

Klynge ressource	
Netværk	

Containerlogs	
VM-ressource	
Node- og serviceadvarsler	

Brugeroprettelse og -administration (RBAC)	

Denne overvågningsløsning er designet til at sikre tryg, effektiv og kompatibel drift af centrale overvågningssystemer i overensstemmelse med FDA's retningslinjer for medicinsk software.

3.2.3 Lagring af logfiler

Systemet gemmer logfiler i ubehandlet (rå) og JSON-format:

- Ubehandlede (rå) logfiler formateres som:

```
{Timestamp}-{Category}-{severity}-{service_timestamp}-{message}
```

- Belastningsjusteringslogs er JSON-formaterede:

```
{
  "log": "{level} {service_timestamp} {caller} {message} {status} {error message}",
  "stream": "stderr",
  "time": "{timestamp}"
}
```

De administrative agenter i Kubernetes-klyngen dirigerer containerens runtime til at skrive applikationsniveau logfiler til mappen, `/var/log/pods`. Kubernetes-klyngens systemniveaulogfiler gemmes også i `/var/lib/rancher/rke2/server/logs`.

Logfilerne her roteres baseret på tilgængelig diskplads. Standard rotationskonfigurationen er:

- audit-log-maxbackup=10 filer
- audit-log-maxsize=100MB.

Logindsamlingsagenten, Promtail, bruger applikationens logfiler `/var/log/pods` fra hver af Kubernetes-noderne og systemniveau-logfilerne `/var/lib/rancher/rke2/server/logs` fra kontrolplannoderne og sendes derefter til Loki, som fungerer som en database for logfiler.

Netværksniveau logfilerne fra belastningsudlignings VM, , gemmes i `/var/lib/docker/containers/` mappe med Promtail-agenten kørende ved siden af, og derefter sendt til Loki.

3.2.4 Håndtering af enhedshændelser

Når der registreres unormale forhold, reagerer systemet i overensstemmelse hermed. Hvis der for eksempel identificeres kontinuerlige loginforsøg, såsom fem på hinanden følgende loginfejl, blokerer systemet for yderligere loginforsøg i 15 minutter.

Alle ukendte enheder uden gyldige certifikater bliver sortlistet og nægtet kommunikation med systemet. Derudover, hvis der registreres for meget netværkstrafik, der påvirker normal drift, stopper systemet datastreaming og underretter slutbrugerne om netværksproblemet via fejlmeddelelser. ANNE Viewing-sessionen mellem sensorerne og ANNE View vil ikke blive påvirket. Disse anomalier overvåges i realtid og logges ved hjælp af det centrale overvågningssystems overvågningsløsning.

3.3 Lokalt MDM-kontrolpanel

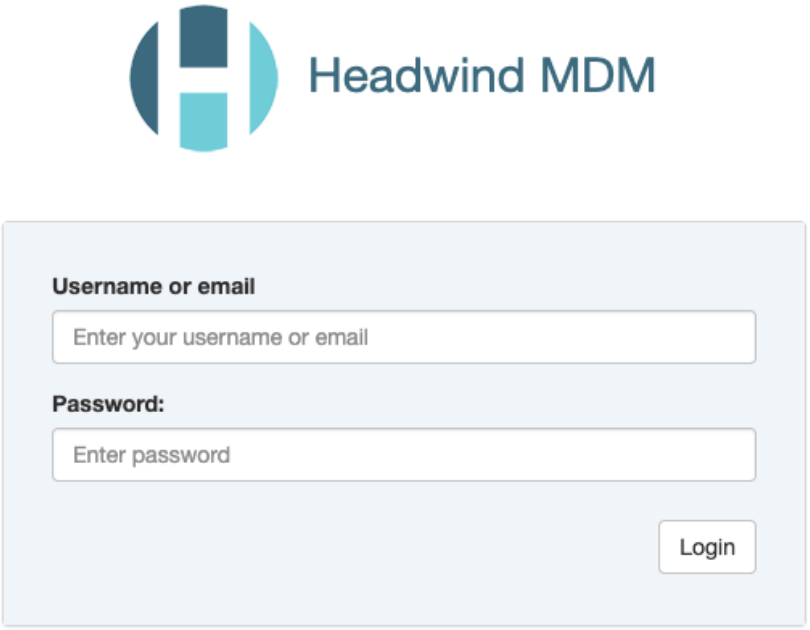
Det lokale MDM-kontrolpanel er tilgængeligt via linket `https://hmdm.${dit-domænenavn}`.

For at få adgang til kontrolpanel-grænsefladen skal den følgende konfiguration være på plads: Der skal oprettes en DNS-post for det angivne domæne via din DNS-udbyder. Uden dette vil kontrolpanel-URL'en ikke blive fortolket korrekt.

Godkendelse:

- Brug den tildelte tekniske bruger-e-mailadresse som brugernavn.
- Standardadgangskoden er: 'admin'.

Ved første vellykkede login vil systemet bede brugeren om at **oprette en ny adgangskode**. Dette er et obligatorisk trin for at fortsætte med yderligere adgang.



Figur 3: Lokal MDM-kontrolpanel logingrænseflade

3.3.1 MDM-licens og enhedsregistrering

For at få adgang til MDM-systemets fulde funktionalitet skal du sørge for, at IT-administratoren har en gyldig licensnøgle. Denne licensnøgle skal anvendes, når CMS-installationen er fuldført og leveret af producenten.

Enhedsregistrering og konfiguration:

Ved hjælp af den lokale MDM-grænseflade vil IT-administratoren kunne:

- Tilmelde ANNE Views ved hjælp af konfigurationsindstillingerne fra Sibel Health.
- Installere Anne-View-applikationen på tilmeldte enheder.
- Aktivere og konfigurere Kiosktilstand for at sikre, at enheden er låst i det tilsigtede kliniske brugsmiljø.

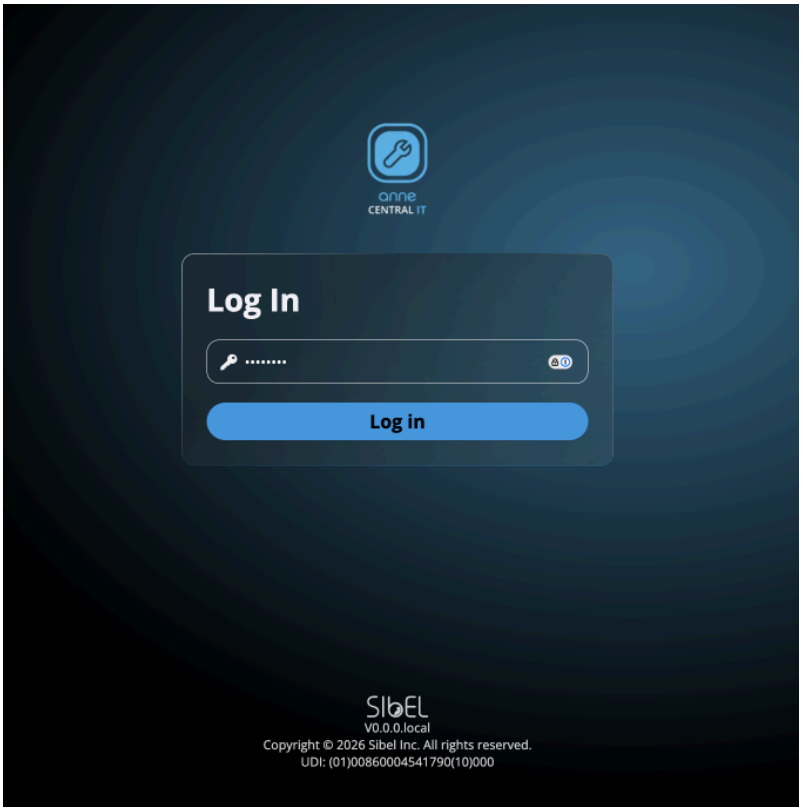
En korrekt licensering og opsætning efter installation er påkrævet for at sikre tryg og stabil enhedsadministration.

3.4 Administrationshub

3.4.1 Login

Admin Hub er tilgængelig via linket `https://cms.${dit-domænenavn}`.

Indtast din adgangskode for at logge ind på Central Hub. Og klik på knappen “Log ind”.



Bemærk: IT-administratoren konfigurerer kontoen og adgangskoden under installationen.

3.4.2 Fejlhåndtering

Tabel 8: Håndtering af loginfejl i Admin Hub

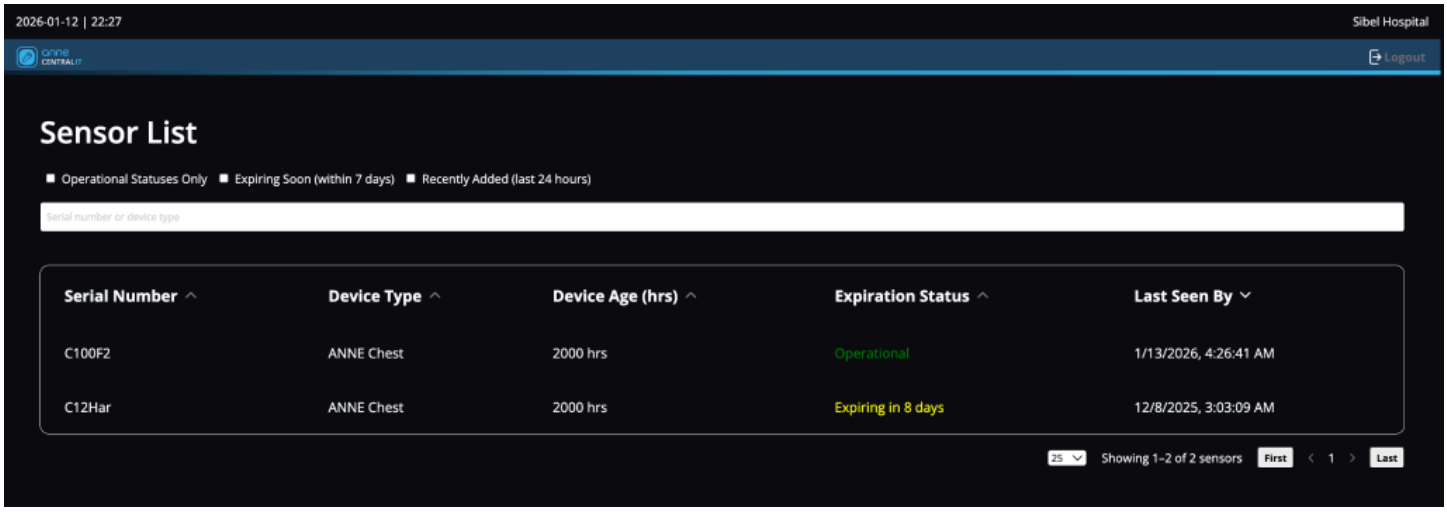
Fejlmeddelelse	Grundliggende årsag:	Anbefalet brugerhandling
Serverfejl: Prøv venligst igen om et par minutter.	Systemets serverfejl.	Prøv igen senere, eller tjek servicestatussen. Hvis problemet fortsætter, skal du kontakte Sibel Health support.
Forkert adgangskode. Prøv venligst igen.	Brugeren indtaster forkert adgangskode.	Prøv igen med den korrekte adgangskode.
Der er blevet prøvet for mange forsøg. Prøv venligst igen om 15 minutter.	Brugeren indtastede en forkert adgangskoden mindst 5 gange.	Prøv igen efter 15 minutter. Hvis du har glemt adgangskoden, skal du nulstille den.

3.4.3 Sensorlevetid-kontrolpanel

Når login er gennemført, vil IT-administratoren kunne:

- Se en liste over de enheder, der er registreret i CMS.
- Admin Hub viser oplysninger såsom serienummer, enhedstype, enhedsalder, udløbsstatus og tidsstempel for sidst set.
- Følgende filtre understøttes for brugervenlighedens skyld: Driftsstatus, udløbsstatus inden for 7 dage, senest tilføjet inden for de sidste 24 timer, serienummer eller enhedstype.
- Enhedens alder og udløbsstatus er muligvis ikke tilgængelig for enheder, der ikke er produceret af Sibel, patientmonitorer og OEM-enheder.

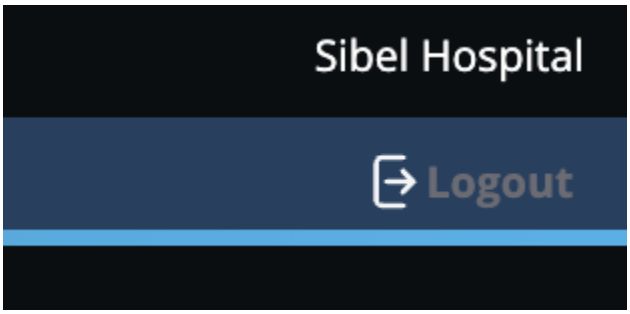
Bemærk: Patientmonitorer og sensorer betegnes her samlet som enheden.



Figur 4: Sensor levetid-kontrolpanel

3.4.4 Log ud

Klik på knappen "Log ud" i øverste højre hjørne.



Bemærk: IT-administratoren logges automatisk ud efter 15 minutters inaktivitet.

Afsnit 4. Vedligeholdelse af centralt overvågningssystem

4.1 Vedligeholdelse af det centrale overvågningssystem

4.1.1 Overvejelser vedrørende cybersikkerhed i forbindelse med det centrale overvågningssystem

Sibel Health har de følgende sikkerhedsovervejelser for installationen af ANNE View og det centrale overvågningssystem for at give det højeste sikkerhedsniveau.

- Godkendelse mellem ANNE View og Central Server bruger X.509-certifikatkæden baseret på certifikater og kædevalidering; kun indgående anmodninger fra ANNE View valideres af den centrale server Det anbefales at generere et certifikat med en udløbsdato på 1 år ved hjælp af openssl med RSA:4096 kryptering.
- Ingen PHI-data vil blive gemt i databasen i det centrale overvågningssystem.
- JSON-webtoken bruges til sikker dataoverførsel mellem det centrale overvågningssystems webportal og backend-gatewayen. Tokenet er gyldigt i 15 minutter, og opdateringstokenet er gyldigt i 7 dage.
- Det centrale overvågningssystem bruger ikke et masternøglelager for at undgå risikoen for brute force, usikker lagring og sidekanalangreb.
- Sibel Health anbefaler, at certifikaternes gyldighedsperioder varierer fra mindst 6 måneder til højst 1 år, hvilket sikrer en balance mellem sikkerhed og driftseffektivitet.

4.1.2 Sikkerhedsrettelser til det centrale overvågningssystem

Eksplicitte programrettelser, der er rettet mod opdagede sårbarheder, er obligatoriske programrettelser og bør opdateres, så snart de modtages. Disse sikkerhedsrelaterede rettelser vil ikke indeholde ny funktionalitet og bør være separate rettelser, der skal implementeres for at beskytte produktet mod sårbarheden.

Når en rettelse er færdiggjort og godkendt, vil Sibel Health distribuere rettelsen til klienterne via et sikkert, hardwarekrypteret USB-drev.

Sikkerhedsrettelser til det centrale overvågningssystem kan installeres af en IT-administrator med adgang til installationen af det centrale overvågningssystem. Trinene for anvendelse af sikkerhedsrettelser til det centrale overvågningssystem er de samme som trinene for opgradering af det centrale overvågningssystem, som er nævnt i afsnit 5 (side 35) i dokumentet SDD-SW-031-007 installationsmanual til det centrale overvågningssystem.

Man kan bekræfte den seneste version ved hjælp af K8s kontrolpanel ved at tjekke billedversionen.

4.1.3 Centrale overvågningssystem rettelser

Programrettelseshastigheden for opdateringer til det centrale overvågningssystem følger en to-ugers sprintcyklus og hotfix-proces. Sibel Health vil sørge for distribution af rettelser.

4.1.4 Version af det centrale overvågningssystem

Der vil blive genereret fulde versioner af Central Monitoring System baseret på Sibel Healths interne udviklingslivscyklus. Versionsudgivelsesprocessen vil følge de korrekte testfaser (verifikation og validering) for at producere en udgivelse bestående af ny funktionalitet, afhjælpning af anomalier fra tidligere udgivelser samt forbedringer af ydeevnen. Distribution af udgivelser vil blive leveret af Sibel Health.

4.1.5 Sikkerhedskopiering og gendannelse af det centrale overvågningssystem

Ved implementering af det centrale overvågningssystem skal databasebackups aktiveres. Denne installation inkluderer ikke integration med ekstern datalagring, og derfor understøttes automatisk databackup ikke. Det er nødvendigt manuelt at sikkerhedskopiere databasen ugentligt som en nød gendannelsesproces.

Backups bør opbevares både på og uden for systemet for at sikre dataredundans og sikkerhed. Backups bør planlægges uden for spidsbelastningsperioder for at minimere påvirkningen af driftsaktiviteter. Regelmæssig overvågning er afgørende for at validere integriteten og pålideligheden af sikkerhedskopierne.

I tilfælde af en kritisk funktionsfejl, kan detaljerede instruktioner til backup/gendannelse findes i afsnit 3.1.3 (side 28) i installationsmanualen til det centrale overvågningssystem SDD-SW-031-007. Sådanne kritiske funktioner ovenfor kan ikke konfigureres af uautoriserede brugere, såvel som beskrivelsen af tilladte kommunikationsporte i afsnit 4.1.

Det centrale overvågningssystem består af et antal virtuelle maskiner, der kører Kubernetes-klyngen. Klyngenoderne gemmer et billede af konfigurationen af hver af noderne i klyngen på ubestemt tid. Som en del af den automatiske gendannelse kører det centrale overvågningssystemtjenester på pods på arbejdsnoder i tilfælde af at en af tjenesterne (pods) går tabt, vil failover og gendannelse via klyngetjenester oprette en erstatning for den mistede pod med dens oprindelige konfiguration, der gendanner klyngen til fuld kapacitet og funktionalitet.

Hvis der opstår et tilfælde, der kræver en manuel gendannelse af en konfigurationskonfiguration, kan en godkendt og autoriseret administrator kopiere konfigurationen fra en anden node for at gendanne klyngens fulde kapacitet og funktionalitet.

4.1.6 Hændelseslogning i det centrale overvågningssystem

Sibel Health tilbyder logging og overvågning af revisionsspor i sine systemer og undersystemer. Disse logfiler og målinger vil give oplysninger om systemernes tilstand, systemernes ydeevnemål samt anomalier eller problemer i systemernes komponenter. Disse hændelser vil være en administrativ funktion og tilgængelige i administrator kontrolpanelet for at kontrollere status, logfiler, målinger og grafer.

Hospitalernes IT-administratorer skal regelmæssigt gennemgå logfilerne via en standardprocedure for kontinuerlig overvågning.

4.1.7 Kryptografisk kontrol af centralt overvågningssystem

Sibel Health skal administrere livscyklussen for nøgler og certifikater via passende kryptografiske moduler såsom 1Password; disse moduler leverer kryptering, adgangskontrol og sikker opbevaring af følsomme data. Alle kryptografiske aktiver vil blive administreret og vedligeholdt af Sibels informationssikkerhedschef i overensstemmelse med anbefalingerne fra NIST SP 800-131A, overgang til brugen af kryptografiske algoritmer og nøglelængder og FIPS 140-3, sikkerhedskrav til kryptografiske moduler.

4.1.7.1 Opbevaring af kryptografiske aktiver

Sibel Health opbevarer og vedligeholder kryptografiske aktiver, nøgler og certifikater i 1Passwords sikre vaults ved hjælp af avancerede krypteringsalgoritmer for at forhindre uautoriseret adgang og ved at sikre kontrolleret adgang kun for autoriseret personale. 1Password sikrer krypteret backup af lagrede aktiver for at understøtte failover-mekanismen.

I tilfælde hvor klienter anmoder om kontrol over kryptografiske aktiver på grund af deres organisations interne cybersikkerhedskrav, vil Sibel Health informere klienter om anvendelse af passende kryptografiske moduler i henhold til bedste praksis for cybersikkerhed, såsom FIPS 140-3, sikkerhedskrav til kryptografiske moduler.

- FIPS 140-3 (FIPS 140-2 afsnit 4.7) beskriver krav vedrørende håndtering af kryptografiske nøgler.

4.1.7.2 Adgangskontrol til kryptografiske aktiver

Alle kryptografiske aktiver skal krypteres, og adgangen skal kontrolleres strengt gennem en rollebaseret adgangskontrol (RBAC)-politik af Sibels udpegede IT/Sikkerhedschef; Sibel Health følger den politikken for adgangskontrol, der anbefales af FIPS 140-3.

Sibel Health vil også give anbefalinger til klienter om udformning af deres politik for adgangskontrol i overensstemmelse hermed. Anbefalingen fra Sibel Health vil tage rollerne og tjenesterne med i betragtningen:

- IT-administrator (superbruger)
    - Fungerer som en superbruger, styrer politikken for adgangskontrol og administrerer livscyklussen for kryptografiske aktiver.
- Sundhedspersonale (bruger)
    - Fungerer som bruger med adgang til de kliniske adgangskoder til det centrale overvågningssystem.

4.1.7.3 Generering og fornyelse af kryptografiske aktiver (rotation)

Kryptografiske nøgler og certifikater genereres før implementeringen og under implementeringen af det centrale overvågningssystem.

De nøgler og certifikater, der kræves før implementeringen, er:

- Digitale signaturnøglepar til både ANNE View og Central Monitoring System-software
- TLS/SSL Certifikatkæde til sikker netværkskommunikation i det centrale overvågningssystem
- Sibels rootCA og IntermediateCA-certifikatkæde til sikker godkendelse og kommunikation mellem ANNE View og Central Monitoring System

På klientens anmodning om sin egen kryptografihåndtering vil Sibel Health give klientens IT-administrator de følgende oplysninger:

- Kryptografialgoritme og protokoller
- Kryptografisk gyldighed

Når kryptografiens gyldighed nærmer sig slutningen, vil Sibel Health forny eller rotere nøglerne og certifikater i henhold til NIST SP 800-57 Del 1, Anbefaling for nøglehåndtering, og NIST 1800-16B, Sikring af webtransaktioner.

Sibel Health vil spore gyldigheden af nøgler og certifikater via kryptografisk modul, 1Password, som vil blive konfigureret til at underrette Sibel Healths IT/Sikkerhedschef eller cybersikkerhedsingeniør 30 dage før nøglerotationen eller certificeringsfornyelsen.

Det anbefales, at klient IT-administratorer udfører nøglerotationen af Central Monitoring System-softwaren i henhold til den kryptoperiode, der er beskrevet i tabel 9.

Tabel 9: Anbefaling af kryptoperiode og certifikatgyldighed pr. aktivtype i henhold til NIST SP 800-57 del 1 og NIST SP 1800-16B

Aktivnavn	Aktivtype	Gyldighed/Kryptoperiode
Nøgle		
Digital signatur	Privat signaturnøgle	1 til 3 år

Digital signatur	Offentlig signatur bekræftelsesnøgle	Ikke specificeret, men følger privat nøgle (1 til 3 år)
Brugergodkendelse	Privat godkendelsesnøgle	1 til 2 år
Brugergodkendelse	Offentlig godkendelsesnøgle	1 til 2 år
Postgres-krypteringsnøgle	Symmetriske datakrypteringsnøgler	3 år
Adgangskode		
Postgres-godkendelsesnøgle	Adgangskode	1 år
Redis-godkendelsesnøgle		
Admin adgangskode		
Admin kontrolpanel-token		
Adgangskode til overvågningskontrolpanelet		
Certifikat		
TLS/SSL Certifikat	Certifikat	1 år
IntermediateCA-certifikat		

Opretholdelse af sikker kommunikation og kryptografi i systemet kræver rettidig fornyelse af certifikater og nøglerotation. Certifikater skal fornys og valideres mindst 30 dage før udløbet af det nuværende certifikat, og nøgler skal roteres i henhold til kryptoperioden. Sibel Health følger NIST SP 1800-16B-vejledningen til fornyelse af certifikater.

Følgende trin beskriver processen for fornyelse af certifikater og levering til klienter:

- **Overvåg certifikatudløb**: Sibel Health IT/Sikkerhedsteamet kontrollerer certifikatets udløbsdato via kryptografimodulet 1Password hver måned. Sibel Health kræver, at klient IT-administratorer rettidigt kontrollerer certifikatudløbet, hvis de selv administrerer certifikater.
- **Generer anmodning om certifikatsignering (CSR)**: Opret en ny CSR til certifikatfornyelsen. Brug eksisterende private nøgler, eller generer nye for at få et nyt certifikat.
- **Indsend CSR til certifikatmyndighed (CA)**: Indsend CSR'en til en betroet CA.
- **Få et nyt certifikat**: Når valideringen er fuldført, vil du modtage det nye sæt af certifikater.
- **Levering af et nyt certifikat**: Sibel Health IT/Sikkerhedsteamet vil dele fornyede certifikater med klient IT-administratorer via 1Password.
- **Udskiftning af et certifikat**: Sibel Health IT/Sikkerhedsteamet kommunikerer med klientens IT-administratorer i nøje overensstemmelse med afsnit 4.5 (side 34) i installationsmanualen til det centrale overvågningssystem SDD-SW-031-007 for at sikre en vellykket udskiftning af certifikatet.
- **Installer certifikatet**: Installer/Udskift det nye certifikat i det centrale overvågningssystem.
- **Genstart tjenester**: Genstart Central Monitoring System-tjenesterne for at anvende det opdaterede certifikat.
- **Bekræft systemfunktionalitet**: Kontroller det centrale overvågningssystem for at sikre, at de nye certifikater fungerer korrekt.

Det er også afgørende for hospitalets IT-administratorer at udføre nøglerotationen af den centrale overvågningssystemsoftware i henhold til instruktionerne i afsnit 4.4 (side 31) i SDD-SW-031-007 installationsmanualen til det centrale overvågningssystem. Sibel Health vil underrette klienter, når nøglerotation skal ske, baseret på systeminstallationens tidslinje og ved hjælp af sikker e-mailkommunikation.

Når nøglerne eller certifikaterne er udskiftet eller roteret til systemet, skal hospitalets IT-administratorer bekræfte det centrale overvågningssystems funktionalitet og drift.

For at sikre, at det centrale overvågningssystem fungerer korrekt:

- **Admin-kontrolpanel IT-administratorvalidering**: Hospitalets IT-administratorer kan verificere infrastrukturens funktionalitet via administrator kontrolpanelet for at sikre, at alle tjenester er operationelle. Et overvågningsværktøj, der er installeret til at understøtte hændelsesdetektion, kan også bruges til validering.
- **Validering af administratorkontrolpanelet**: Hospitalets IT-administratorer kan verificere systemets grundlæggende funktionalitet ved at kontrollere brugergodkendelse og sikre, at systemet udfører sin tilsigtede funktion korrekt.

4.1.7.4 Tilbagekaldelse af kryptografiske aktiver

I tilfælde af nøgle/certifikat kompromis,

- tilbagekaldelse af nøgle
- genudstedelse
- omkonfiguration

I tilfælde af at en nøgle eller et certifikat der er kompromitteret opdages eller overskrides udløbs- eller kryptoperioden, skal Sibel Healths IT/Sikkerhedsteam reagere med øjeblikkelige handlinger, herunder tilbagekaldelse af nøgler, genudstedelse og omkonfiguration af berørte systemer, og opfordre klienter til at træffe øjeblikkelige foranstaltninger for at afbøde sikkerhedsrisici.

Processen skal følges som beskrevet i afsnit 4.1.7.3, generering og fornyelse af kryptografiske aktiver (rotation):

- Generering af kryptografi
- Tilbagekaldelse af nøgle
- Genudstedelse af kryptografi
- Udskiftning
- Verifikation af drift

4.1.7.5 Kryptografiske aktiver sletning/destruktion

For kryptografiske nøgler eller certifikater, der ikke længere er i brug, skal Sibel Healths IT/Sikkerhedschef destruere ubenyttede kryptografiske aktiver og foretage uoprettelige sletninger fra kryptografimodulet. Dette forhindrer enhver mulighed for at gendanne eller rekonstruere kryptografiske nøgler eller følsomme data. Sibel Health følger vejledningen i NIST SP 800-88, som indeholder standarder for sikker datarensning.

Sibel Healths IT/Sikkerhedschef skal bekræfte, at klientens IT-administratorer følger de samme protokoller for at sikre nulstilling af kryptografiske aktiver.

4.2 Nedlukning af centralt overvågningssystem (EOL)

4.2.1 Version af centralt overvågningssystem understøttes ikke længere

Versionerne af det centrale overvågningssystem understøttes op til to versioner bagud, men når en version ikke længere understøttes, vil klienter blive instrueret i opgraderingsstien til den nyeste version. Brugere, der fravælger opgraderinger, vil ikke længere modtage opdateringer (sikkerhed eller programrettelser). Sibel Health vil udarbejde

oplysninger om kendte sårbarheder til klienter for at informere dem om risiciene ved ikke at skifte til den nyeste version.

4.2.2 Det centrale overvågningssystems levetids ophør

Når det centrale overvågningssystem når sit slutscenarie, vil Sibel Health informere alle kunder om den dato, hvor der ikke længere vil være support eller forventning om pålidelig brug af systemet. Sibel Health har udarbejdet et dokument, SDD-SW-031-007 Central Monitoring System Installation Manual, der indeholder nedlukningsprocedurerne i afsnit 6 (side 37) for sikkert at fjerne applikationen fra dens installerede placering samt muligheder for datasletning.

Bemærk venligst, at følsomme oplysninger kan blive eksponeret, hvis systemet tages ud af drift forkert eller ufuldstændigt:

- For- og efternavn
- Fødselsdato
- Patient ID

Afsnit 5. Fejlfinding

5.1 Validering af forbindelsen til Kubernetes API

```
kubectl get no


# the output should be similar to the below
NAME       STATUS   ROLES                       AGE   VERSION
master-1   Ready    control-plane,etcd,master   23d   v1.30.8+k3s1
```

Hvis denne fejlmeddelelse vises:

```
“The connection to the server localhost:8080 was refused - did you specify the right host or port?”
```

Det betyder, at konfigurationsfilen mangler i standardindstillingen. `~/.kube` placeringen. Kontroller at filen er kopieret fra installationsplaceringen til standardplaceringen, og prøv igen. Filen skal være præcist konfigureret og være placeret i `~/.kube` mappen.

For at forenkle kommunikationen med Kubernetes-klyngefilen, skal ‘~/sibel-install/kubeconfig’ kunne kopieres til ‘~/.kube’ mappen med navnet config, som er en placering, som kubectl kontrollerer og bruger som standard.

```
mkdir -p ~/.kube
cp ~/sibel-install/kubeconfig ~/.kube/config
```

Filen `~/.kube/config` skal ligne:

```
apiVersion: v1
clusters:
- cluster:
    certificate-authority-data: <REDACTED>
    server: https://<K8S-API-ADDRESS>:6443
  name: default
contexts:
- context:
    cluster: default
    namespace: central-hub
    user: default
  name: dev@cluster.local
current-context: dev@cluster.local
kind: Config
preferences: {}
users:
- name: default
  user:
    client-certificate-data: <REDACTED>
    client-key-data: <REDACTED>
```

5.2 Fejl i installation af centralt overvågningssystem

Under installationsprocessen kan du støde på de følgende fejl eller noget tilsvarende:

```
k8s-api.control-lb.qa.tucana.sibel.health on 192.168.65.7:53: no such host
```

I de fleste tilfælde betyder det, at trinnet med at oprette DNS-poster fra installationsmanualen er blevet sprunget over. DNS-posterne er nødvendige for at komponenterne i det centrale overvågningssystem kan kommunikere med hinanden. DNS-posterne skal oprettes i DNS-udbyderen for det domæne, der bruges til implementeringen af det centrale overvågningssystem, og også for Kubernetes API-domænet.

DNS-posterne skal oprettes for de følgende domæner:

```
- domain name for the Kubernetes API, should be pointing to the IP address of the load
balancer that was created during the VMs setup. E.g. `k8s-api.hq.tucana.sibel.health` >
`192.168.1.81` (IP of the VM with  load balancer for Kubernetes API)

- domain name for the Central Hub API, should be pointing to the IP address of the load
balancer that was created during the VMs setup. E.g. `api.hq.tucana.sibel.health` >
`192.168.1.81` (IP of the VM with load balancer for Central Hub API)

- domain name for the Central Hub CMS, should be pointing to the IP address of the load
balancer that was created during the VMs setup. E.g. `cms.hq.tucana.sibel.health` >
`192.168.1.81` (IP of the VM with load balancer for Central Hub UI)
```

Som en løsning for Kubernetes API-domænet kan du tilføje følgende linje til `/etc/hosts`-filen på den maskine, hvor installationen udføres:

```
k8s-api.control-lb.qa.tucana.sibel.health <IP of the VM with HAproxy loadbalancer for K8S
API>
```

5.3 Fejl i centralt overvågningssystem

Hvis det centrale overvågningssystem ikke fungerer som forventet, kan følgende trin foretages for at finde en forklaring på problemet:

1. Kontroller status for komponenterne i det centrale overvågningssystem ved hjælp af den følgende kommando:

```
kubectl get po -n central-hub

# the output should be similar to the below
NAME                                          READY   STATUS      RESTARTS        AGE
auth-7d9cccc69f-btbmh                                 1/1     Running       1 (7d12h
ago)      15d
backup-postgres-29442300-whs6v                        0/1     Completed     0
2d3h
backup-postgres-29443740-b24f8                        0/1     Completed     0
27h
backup-postgres-29445180-j26mp                        0/1     Completed     0
3h23m
```

```
central-monitoring-769845f97c-f9cjl                    1/1     Running       1 (7d12h
ago)      15d
fleet-manager-6b785587d9-p5wgz                         1/1     Running       1 (7d12h
ago)      15d
hmdm-headwind-mdm-55dd666cd-6hflq                      1/1     Running       2
15d
postgres-1-0                                           1/1     Running       2
15d
redis-0                                                1/1          Running       1
(7d12h ago)      15d

               5d20h
```

Alternativt kan du gøre det samme ved hjælp af Kubernetes-kontrolpanelet. Log ind på kontrolpanelet og naviger til `central-hub` navneområdet og tjek status for pods på `Workloads`-siden.

2. Hvis der er pods, der ikke er `Kører` eller `Afsluttet`, tjek pod'ens logfiler for at identificere problemet. Logfilerne kan kontrolleres ved hjælp af den følgende kommando:

```
kubectl logs -n central-hub <pod-name>
```

Eller ved at bruge Kubernetes-kontrolpanelet. Naviger til `central-hub` navneområdet og tjek logfilerne for pod'en på `Workloads`-siden.

3. Hvis nogle af pod'erne er i `Pending` tilstand, tjek podens hændelser for at identificere problemet. Hændelserne kan kontrolleres ved hjælp af den følgende kommando:

```
kubectl describe po -n central-hub <pod-name>
```

Eller ved at bruge Kubernetes-kontrolpanelet. Naviger til `central-hub` navneområdet og tjek podens hændelser på `Workloads`-siden.

Hændelser er normalt selvforklarende og kan hjælpe med at identificere problemet.

En mulig årsag til de afventende pods kan være, at den node, hvor poden skal planlægges, ikke er klar, eller at der ikke er nok ressourcer på noden til at planlægge poden.

Nodens status kan kontrolleres ved hjælp af den følgende kommando:

```
kubectl get no

# the output should be similar to the below
NAME       STATUS   ROLES                       AGE   VERSION
master-1   Ready    control-plane,etcd,master   28d   v1.30.8+k3s1
```

Hvis en af noderne ikke er `Ready`, kontroller hændelserne og nodens tilstand for at identificere problemet ved hjælp af den følgende kommando:

```
kubectl describe no <node-name>
```

Læs outputtet omhyggeligt for at identificere eventuelle problemer med noden.

5.4 URL'en til det centrale overvågningssystem er ikke tilgængelig

Hvis URL'en til det centrale overvågningssystem ikke er tilgængelig, kan de følgende trin udføres for at finde frem til forklaringen på problemet:

1. Kontroller at DNS-posten findes for URL'en til det centrale overvågningssystem hos din DNS-udbyder. Den korrekte IP-adresse er IP-adressen på den load balancer, der blev oprettet under installationsprocessen.
2. Hvis DNS-posten findes, er næste trin at kontrollere, om adgangs-controlleren i Kubernetes-klyngen fungerer korrekt. Adgangs-controlleren er ansvarlig for at dirigere trafikken til den korrekte tjeneste i Kubernetes-klyngen. For at kontrollere status for adgangs-controlleren skal du bruge den følgende kommando:

```
kubectl get po -n ingress-nginx

# the output should be similar to the below
NAME                                        READY   STATUS    RESTARTS        AGE
ingress-nginx-controller-7fb9dccf4d-sxzkr   1/1     Running   2 (7d12h ago)   15d
ingress-nginx-defaultbackend-5b4d94fcdd-qptqb   1/1     Running   1 (7d12h ago)   15d
```

Hvis alle pods er i `Running` tilstand, tjek logfilerne for adgangs-controlleren for at identificere problemet ved hjælp af den følgende kommando:

```
kubectl logs -l app.kubernetes.io/instance=ingress-nginx -n ingress-nginx -f
```

Ovenstående kommando vil følge logfilerne for adgangs-controller pods og vise logfilerne i realtid. Prøv at oprette forbindelse til URL'en, og tjek logfilerne for fejl.

Du kan bruge `grep` under logfilerne, kontroller for at undersøge det specifikke værtsnavn, der ikke er tilgængeligt, for at identificere problemet. Hvis logfilerne for værtsnavnet findes i logfilerne, ligger problemet højst sandsynligt i de komponenter i det centrale overvågningssystem, der modtager trafikken.

3. Kontroller, at central-hub adgangen skal oprettes med port 443, som vist nedenfor.

```
root@ee659bc0fd71:/install# kubectl -n central-hub get ingress central-monitoring
NAME                 CLASS   HOSTS                          ADDRESS         PORTS     AGE
central-monitoring   nginx   cms.hq.tucana.sibel.health   192.168.7.242   80, 443   6d1h
```

4. Hvis den er oprettet, så tjek om central-hub-tls-hemmeligheden skal oprettes

```
root@ee659bc0fd71:/install# kubectl -n central-hub get secret central-hub-tls
NAME              TYPE                DATA   AGE
central-hub-tls   kubernetes.io/tls   2      6d1h
```

5. Tjek logfilerne over de defekte komponenter i det centrale overvågningssystem for at identificere problemet ved hjælp af den følgende kommando:

```
kubectl logs -n central-hub <pod-name>
```

ANNE View kan ikke oprette forbindelse til det centrale overvågningssystem

5.5 ANNE View kan ikke oprette forbindelse til det centrale overvågningssystem

1. Kontroller at ANNE View har gyldige SDC-certifikater.
2. Kontroller at ANNE View og Central Monitoring System er på det samme netværk.

3. Tjek logfilerne for fleet-manager pods i klyngen for at identificere en mulig årsag til problemet.

```
kubectl logs -l app.kubernetes.io/instance=fleet-manager -n central-hub -f
```

Ovenstående kommando vil følge logfilerne fra SDC-pod'ene og vise logfilerne i realtid. Prøv at forbinde ANNE View til det centrale overvågningssystem og tjek loggene for eventuelle fejl.

5.6 Forbindelsesproblemer mellem pods i klyngen, mens pods kører på forskellige noder

1. Kubernetes-klynger bruger overlay-netværket til at forbinde pods, der kører på forskellige noder. Overlay-netværket oprettes af CNI-plugin'et, der er installeret på klyngen. CNI-pluginnet er ansvarlig for at oprette netværket og administrere netværkstrafikken mellem podsene.
2. Hvis podsene ikke kan kommunikere med hinanden, skal du først kontrollere nodernes status ved hjælp af den følgende kommando:

```
kubectl get no

# the output should be similar to the below
NAME       STATUS   ROLES                       AGE   VERSION
master-1   Ready    control-plane,etcd,master   23d   v1.30.8+k3s1
```

3. Hvis noderne er `Ready`, Tjek status for CNI-pods ved hjælp af den følgende kommando:

```
kubectl get po -n kube-system -l app.kubernetes.io/part-of=cilium -owide
# the output should be similar to the below
NAME                                          READY   STATUS    RESTARTS        AGE
IP           NODE     NOMINATED NODE   READINESS GATES
coredns-7f6545b9bb-6rrsx                      1/1     Running   1 (7d12h ago)   15d
10.42.0.52   l3s-cl   <none>           <none>
local-path-provisioner-595dcfc56f-9478f       1/1     Running   0               7d12h
10.42.0.55   l3s-cl   <none>           <none>
metrics-server-cdcc87586-vjml9                1/1     Running   3 (7d12h ago)   15d
10.42.0.59   l3s-cl   <none>           <none>
svclb-ingress-nginx-controller-f38bdbb0-jpgmt   5/5     Running   6 (7d12h ago)   15d
10.42.0.50   l3s-cl   <none>           <none>
```

Hvis podsene ikke er i `Drift` tilstand, tjek pod'ens logfiler for at identificere problemet ved hjælp af den følgende kommando:

```
kubectl logs -n kube-system <pod-name>
```

5.7 Ændring af klynge IP-adresser efter genstart af serveren

ADVARSEL: Der bør træffes forholdsregler for at undgå ændring af IP-adresserne på noderne i Kubernetes-klyngen efter genstarten af serveren. Kontroller at de IP-adresser, der er tildelt Kubernetes-klyngenoderne, er statiske og ikke er tildelt af DHCP-serveren i netværket.

Hvis IP-adresserne på noderne i Kubernetes-klyngen ændres efter genstarten af serveren, skal Kubernetes-klyngen nulstilles med de nye IP-adresser. De følgende trin skal foretages for at nulstille Kubernetes-klyngen med de nye IP-adresser:

1. Opret forbindelse til kontrolplannoden i Kubernetes-klyngen ved hjælp af SSH.
2. Opret 'k3s_backup' mappen

```
mkdir ~/k3s_backup
```

3. Kopier k3s binærfil og installer scriptet til k3s_backup

```
cp /usr/local/bin/k3s ~/k3s_backup/
```

4. Stop k3s-tjenesten

```
Kubectl stop k3s
```

5. Kør nedenstående script for først at fjerne k3'er

```
sh /usr/local/bin/k3s-killall.sh

sh /usr/local/bin/k3s-uninstall.sh
```

6. Installer nu k3'erne med den nye IP-adresse

INSTALL_K3S_SKIP_DOWNLOAD=true K3S_DATA_DIR=/data/var/lib/rancher/k3s \

INSTALL_K3S_EXEC="server –deaktiver traefik --node-ip {{ NEW_IP }} --annoncér-adresse {{ NEW_IP }}" \

./tmp/install-k3s.sh

7. Kontroller status for klyngenoder

```
root@k3s-single-node:/home/sibel# kubectl get nodes
NAME            STATUS   ROLES                       AGE     VERSION
k3s-server-01   Ready    control-plane,etcd,master   5d17h   v1.30.8+k3s1
```

Afsnit 6. Offentliggørelse af sårbarheder

6.1 Sibel Sundhedspolitik for oplysning om sårbarheder

Som leverandør af sikker software, tjenester og forskning tager kundesupportrepræsentanten sikkerhedsproblemer alvorligt og anerkender vigtigheden af privatliv, sikkerhed og opsøgende arbejde i lokalsamfundet. Derfor er kundesupportrepræsentanten forpligtet til at håndtere og rapportere sikkerhedsproblemer. Denne politik beskriver, hvordan man rapporterer sårbarheder, hvad man kan forvente som reaktion, og hvordan kundesupportrepræsentanten vil håndtere dem.

6.2 Rapportering af sikkerhedsproblemer

Hvis du mener, at kundesupportmedarbejderen har opdaget en sårbarhed i et produkt, eller hvis du har et sikkerhedsproblem, du gerne vil rapportere, bedes du rapportere det ved at følge disse trin:

- **E-mail**: Send en detaljeret rapport til security@sibelhealth.com. Hvis du føler behov for det, bedes du bruge vores offentlige PGP-nøgle nedenfor til at kryptere din kommunikation med os.
    - Offentlig PGP-nøgle

```
-----BEGIN PGP PUBLIC KEY BLOCK-----

mDMEZt+KghYJKwYBBAHaRw8BAQdAi5TvQjkUR+3OeAwyRzck68CXwJB48cyT2agM
QDJlp4a0LEpvbmcgWW9vbiBMZWUgPGpvbmd5b29uLmxlZUBzaWJlbGhlYWx0aC5j
b20+iJMEExYKADsWIQSr1EgI/KSP5svTwCruWcLTCBvB8QUCZt+KggIbAwULCQgH
AgIiAgYVCgkICwIEFgIDAQIeBwIXgAAKCRDuWcLTCBvB8XQlAQDd4uf8JftUfefR
GLOC2nKNkyEvHTfxghCFrGTCl1GXLQEAmleqy8ZNKUqdb2dO0SvxnQtNqmFyNe1M
pklTAPJVfgi4OARm34qCEgorBgEEAZdVAQUBAQdAGM5w5lJozi/X8rJP6xmIvP5t
uJ8Xc0b/s6slT+ZfKRADAQgHiHgEGBYKACAWIQSr1EgI/KSP5svTwCruWcLTCBvB
8QUCZt+KggIbDAAKCRDuWcLTCBvB8Z9HAQCwDhcB8kCZQxxSyPLEon6mL+HB8leD
R49iMPOmdkyeDAD+Ku1Of1fUSP4e/ShmtcnjEF7d7RcA+NqbNAOLtWztIwg=
=F/DG
-----END PGP PUBLIC KEY BLOCK-----
```

- **Oplysninger, der skal medtages:**
    - En detaljeret beskrivelse af sårbarheden, herunder
        - Produkt- eller tjenestenavn, URL og berørte versioner.
        - Operativsystem for involverede komponenter.
        - Softwarekonfiguration af computeren eller enheden på tidspunktet for registrering.
        - Klasse eller type af sårbarhed (f.eks. ved brug af en taksonomi såsom CWE).
        - Tidspunkt og dato for opdagelsen.
    - Trin til at reproducere problemet
        - Teknisk beskrivelse af udførte handlinger, rækkefølge og resultat.
        - PoC code/Værktøjer anvendt til at fremstille den sårbare adfærd.
    - Potentiel påvirkning og estimat af alvorlighed, hvis tilgængelig.
    - Potentiel grundårsag, hvis tilgængelig.

- Vurdering af omfang, andre produkter, komponenter, tjenester eller leverandører, der menes at være berørt, hvis tilgængelig.
- Offentliggørelsesplaner, specifikt embargo- og offentliggørelsestidslinjer, hvis tilgængelige.

6.3 Vores forpligtelse

Når en sårbarhed rapporteres til kundesupportrepræsentanten, forpligter vi os til at:

- Bekræftelse på modtagelse af din rapport inden for 7 hverdage.
- Vurder og verificer legitimiteten af sårbarheden.
- Kategoriser alvorligheden af sårbarheden baseret på potentiel påvirkning.
- Udvikl en afhjælpningsplan baseret på alvoren og iværksæt en løsning.
- Angiv en estimeret tidslinje for afhjælpning.
- Kommunikation af fremskridt gennem hele afhjælpningsprocessen via e-mail
- Rådgivende kommunikation med afhjælpning i henhold til vores interne procedure for sårbarhedsstyring.
- Behandle hver rapport fortroligt og ikke videregive den til tredjeparter uden samtykke.
- Oplys sårbarheder i udgivelsesnoter til opdateringer.

Bemærk venligst, at ikke alle problemer vil være omfattet af Sibels sårbarhedsoplysningsproces, herunder:

- Rapporter om manglende sikkerhedsheadere, der ikke fører til betydelig påvirkning eller forringelse af ydeevnen.
- Forældede platformsspecifikke problemer.
- Sociale tekniske angreb eller fysiske sårbarheder (f.eks. kontorsikkerhed).
- Problemer med tredjepartstjenester, der ikke håndteres af kundesupportrepræsentanten

Afsnit 7. Bilag

7.1 Maskinlæsbar SBOM

```
1,2,3,4,Unique Identifier,Component Name,Author Name,Supplier
Name,Timestamp,Version,Component Hash (Optional),Relationship,License,Level of Support,End
of Service

X,,,,,Central Hub,,,,2.1.0,,Primary,,,
,X,,,SOUP-017,React,Naeem Bobada,Meta,9/2/2025,19.0.3,N/A,Included in,MIT license,Actively
Maintained,N/A
,X,,,SOUP-080,Lodash,Jeff Lee,Lodash Utilities,8/16/2024,4.17.21,N/A,Included in,MIT
License,Actively Maintained,N/A
,X,,,SOUP-081,Emotion,Jeff Lee,Emotion,8/16/2024,11.10.6,N/A,Included in,MIT
License,Actively Maintained,N/A
,X,,,SOUP-084,Next.js,Medhat Ibrahim,Vercel,9/2/2025,15.5.2,N/A,Included in,MIT
License,Actively Maintained,N/A
,X,,,SOUP-118,Javascript,Jeff Lee,ECMA International,8/16/2024,ECMAScript
2015,N/A,Included in,ECMA standard,Actively Maintained,N/A
,X,,,SOUP-119,Typescript,Jeff Lee,Microsoft,8/16/2024,5.1.6,N/A,Included in,Apache
2.0,Actively Maintained,N/A
,X,,,SOUP-123,Node.js,Naeem Bobada,Node.js,9/2/2025,24.5.0,N/A,Included in,MIT
License,Actively Maintained,4/30/2028
,X,,,SOUP-147,react-i18next,Ignacio Duran,18next ecosystem,9/2/2025,15.0.2,N/A,Included
in,MIT License,Active Maintenance,N/A
,X,,,SOUP-148,Zod,Naeem Bobada,colinhacks community,9/2/2025,4.1.11,N/A,Included in,MIT
License,Active Maintenance,N/A
,X,,,SOUP-146,React-dom,Naeem Bobada,"Meta Platforms, Inc",9/2/2025,19.0.3,N/A,Included
in,MIT License,Active Maintenance,N/A
,X,,,SOUP-156,dayjs,Harshit Shah,Iamkun,1/14/2026,1.11.19,N/A,Included in,MIT
License,Active Maintenance,N/A
,X,,,SOUP-157,ffi-rs,Harshit Shah,zhangyuang,1/14/2026,1.3.1,N/A,Included in,MIT
License,Active Maintenance,N/A
,X,,,SOUP-158,zustand,Harshit Shah,Poimandres,1/14/2026,5.0.9,N/A,Included in,MIT
License,Active Maintenance,N/A

X,,,,,Central Server,,,,2.1.0,,Primary,,,
,X,,,SOUP-062,FastAPI,Jeff Lee,FastAPI,8/16/2024,0.115.5,N/A,Included in,MIT
License,Actively Maintained,N/A
,X,,,SOUP-063,Pydantic,Badal Mishra,Pydantic,9/2/2025,2.8.1,N/A,Included in,MIT
License,Actively Maintained,N/A
,X,,,SOUP-064,Uvicorn,Jeff Lee,Encode,8/16/2024,0.24.0,N/A,Included in,BSD
3-Clause,Actively Maintained,N/A
,X,,,SOUP-066,asyncpg,Badal Mishra,MagicStack,9/2/2025,0.30.0,N/A,Included in,Apache
Software License,Actively Maintained,N/A
```

,X,,,SOUP-068,Httpx,Jeff Lee,Encode,8/16/2024,0.25.2,N/A,Included in,BSD License,Actively Maintained,N/A
,X,,,SOUP-069,Sqlalchemy,Badal Mishra,Sqlalchemy,9/2/2025,2.0.42,N/A,Included in,MIT License,Actively Maintained,N/A
,X,,,SOUP-070,Loguru,Jeff Lee,Active Maintenance,8/16/2024,0.7.2,N/A,Included in,MIT License,Actively Maintained,N/A
,X,,,SOUP-071,Pyjwt,Jeff Lee,Pyjwt,8/16/2024,2.10.1,N/A,Included in,MIT License,Actively Maintained,N/A
,X,,,SOUP-097,Redis,Jeff Lee,Redis,8/16/2024,6.2.14-bookworm,N/A,Included in,RSALv2),No Longer Maintained,12/31/2025
,X,,,SOUP-098,Kubernetes,Jeff Lee,Cloud Native Computing Foundation,8/16/2024,1.30.8-rke2r1-build20241212,N/A,Included in,Apache 2.0,No Longer Maintained,N/A
,X,,,SOUP-099,Apache Kafka,Jeff Lee,Apache Software Foundation,8/16/2024,3.7.1,N/A,Included in,Apache 2.0,Actively Maintained,7/26/2026
,X,,,SOUP-100,PostgreSQL,Jeff Lee,PostgreSQL,8/16/2024,14.12,N/A,Included in,PostgreSQL License,Actively Maintained,11/12/2026
,X,,,SOUP-122,Ubuntu,Keneel Gajera,Canonical Ltd.,9/2/2025,24.04.2 LTS,N/A,Included in,"Various (GPL, etc.)",Actively Maintained,4/1/2027
,X,,,SOUP-121,Alpine Linux,Jeff Lee,Alpine Linux,8/27/2024,3.19.1,N/A,Included in,MIT License,Actively Maintained,11/1/2025
,X,,,SOUP-116,Python,Badal Mishra,Python Software Foundation,9/2/2025,3.13.5,N/A,Included in,PSF License,Actively Maintained,10/1/2029
,X,,,SOUP-141,Argon2,Keneel Gajera,Argon2,9/2/2025,23.1.0,N/A,Included in,General Public License v3.0,Actively Maintained,N/A
,X,,,SOUP-143,cryptography,Mathias Lantean,PyCA,9/2/2025,44.0.0,N/A,Included in,Apache-2.0 OR BSD-3-Clause,Actively Maintained,N/A
,X,,,SOUP-144,psycopg2-binary,Roshani Vasava, psycopg/psycopg2 community,9/2/2025,2.9.10,N/A,Included in,LGPL-3.0-or-later,Actively Maintained,N/A
,X,,,SOUP-145,pydantic-settings,Roshani Vasava,Pydantic Team,9/2/2025,2.3.0,N/A,Included in,MIT License,Actively Maintained,N/A
,X,,,SOUP-159,markupsafe,Harshit Shah,Pallets Projects team,1/14/2026,2.1.3,N/A,Included in,BSD-3-Clause License,Actively Maintained,N/A
,X,,,SOUP-160,HeadwindMDM,Jeff Lee,Headwind Solutions,1/23/2026,5.37.4,N/A,Included in,Commercial,Actively Maintained,N/A