SIbEL

CENTRAL hub

BRUKSANVISNING

ANNE One Admin

support.sibelhealth.com

IFU P/N 443-00006-SV-A

Innehållsförteckning

Avsnitt 1. Viktig säkerhetsinformation

1.1 Översikt

Detta dokument är avsett för kvalificerad teknisk personal som ansvarar för installation, konfiguration, underhåll och service av ANNE One-systemet från den administrativa hubben och dess nätverksanslutna komponenter. Den beskriver inte klinisk eller patientnära användning.

Tillåtna serviceaktiviteter inkluderar:

- Installation och konfiguration av systemets programvara och stödjande infrastruktur enligt beskrivningen i denna IFU och tillhörande installationsmanualer och SDD-SW-031-007 installationsmanual för centralt övervakningssystem.
- Övervakning av systemet, granskning av loggar, säkerhetskopiering, återställning, patchning och avveckling beskrivs uttryckligen i detta dokument.
- Konfiguration av nätverk, server och åtkomstkontroll i enlighet med de rekommendationer som anges.

Förbjudna handlingar inkluderar:

- Modifiering av programvara, firmware, systemarkitektur, säkerhetskontroller och konfigurationer som avviker från dokumenterade förfaranden.
- Användning av odokumenterade gränssnitt, inloggningsuppgifter och bakdörrsmekanismer.
- Serviceaktiviteter som kan förändra klinisk funktionalitet, datas integritet eller efterlevnad av regelverk.

Tillverkarens godkännande krävs för:

- Alla avvikelser från dokumenterade förfaranden för installation, uppgraderingar, patchningar, återställningar och förfaranden för cybersäkerhet.
- Manuella interventioner i databaser, containrar eller operativsystem om inte dessa uttryckligen beskrivs i denna IFU eller servicedokumentation från tillverkaren.

1.2 Ordlista

Tabell 1: Ordlista

Förkortning	Definition
IFU	Bruksanvisning (Instructions For Use)
RBAC	Rollbaserad åtkomstkontroll (Role-Based Access Control)
ADT	Inskrivning, Utskrivning, Överföring (Admission, Discharge, Transfer)
PM	ANNE View
BLE	Bluetooth lågenergi (Bluetooth Low Energy)
EOL	Produkten uttjänt (End of Life)

NFC	Närfältskommunikation (Near Field Communication)
LED	Lysdiod
IP	Inträngningsskydd
IT	Informationsteknik
VM	Virtuell Maskin
TPM	Tillförlitliga PlattformsModuler

1.3 Symboler

Tabell 2: Symboler

Symbol	Titel	Beskrivning
Rx ONLY	Endast receptbelagt bruk	Enligt federal lag får denna enhet endast säljas av eller på ordination av licensierad sjukvårdspersonal
	Se instruktionsmanual/häfte	Anger att instruktionsmanualen/häftet måste läsas
	eIFU	Anger att användare behöver konsultera bruksanvisningen eller den elektroniska bruksanvisningen.
QTY	Kvantitetssymbol	Anger antalet enheter eller stycken i paketet.
EC REP	Auktoriserad representant i Europeiska unionen	Anger den auktoriserade representanten i Europeiska unionen.
CE 2460	CE-märkning	Anger att en produkt har utvärderats av tillverkaren och bedömts uppfylla EU:s säkerhets-, hälso- och miljöskyddskrav. Det krävs för produkter som marknadsförs i EU oavsett var i världen de är tillverkade.

1.4 Information om tillverkare

- Kontakta representanten på kundsupporten vid något av följande problem:
    - Hjälp med att konfigurera, använda eller underhålla det centrala övervakningssystemet
    - För att rapportera oväntade operationer eller händelser

Sibel Health Inc.
Adress: 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

Avsnitt 2. Produktspecifikationer

2.1 Produktspecifikationer

Tabell 3: Specifikationer för det centrala övervakningssystemet

	Centralt övervakningssystem (server)
CPU	1 × 4-kärnig CPU @ 2,4 GHz
RAM	6 GB
Hårddisk, storlek	Disk för operativsystem – 100 GB Datadisk – 300 GB SSD
Extern lagring	Ingen
Nätverk	100/1000 Mbit/s Ethernet
Annan hårdvara	Avbrottsfri strömförsörjning (UPS)
Operativsystem	Ubuntu 24.04 Noble Numbat
Stödjande programvara	Ingen

Tabell 4: Specifikationer för det centrala övervakningssystemets USB-minne

Märke	iStorage
Modellnummer	IS-FL-DA3C-256-32
Lagringskapacitet	32 GB
Gränssnitt	USB typ C med adapter typ A
Dataöverföringshastighet	Läsning: 310 MB/s Skrivning: 246 MB/s
Mått (mm)	Höjd: 80,10 mm Bredd: 20,25 mm Djup: 10,70 mm
Vikt	25 g
Operativsystemets kompatibilitet	MS Windows, macOS, Linux, Chrome, Android, Tunna klienter, Nollklienter, Inbyggda system, Citrix och VMware
Krypteringsnycklar	256-bitars hårdvarukryptering

2.2 Säkerhetsrekommendationer

- Se till att aktivera diskkryptering för operativsystemets disk för att stödja datasäkerheten.
- Använd TPM eller säker boot före installationen.
- Använd antivirus- eller antimalware-verktyg på värdarna före installationen.
- Kommunikation mellan tredje parts applikationer och komponenten i det centrala övervakningssystemet kan endast ske om tredje parts applikationens käll-IP-adress är vitlistad.
- Det centrala övervakningssystemet använder inte en huvuddatabas för lagring av nycklar för att undvika risken för brute force-attacker, osäker lagring och attacker på sidokanaler.
- Regelbunden övervakning och säkerhetskopiering av data rekommenderas.
- Använd begränsningar för användning av fysiska eller bärbara enheter på det centrala övervakningssystemets server samt på det Windows-system som ska användas för övervakning.

2.3 Rekommendationer för nätverk

- Se till att både PMS och det centrala övervakningssystemet är anslutna till samma lokala nätverk (LAN) eller VLAN.
- Konfigurera brandväggar till att strypa nätverket för användare som upptäcks med ont uppsåt. Stryp användarna till 10 megabits/second och meddela IT-administratörer om skadliga aktörer.

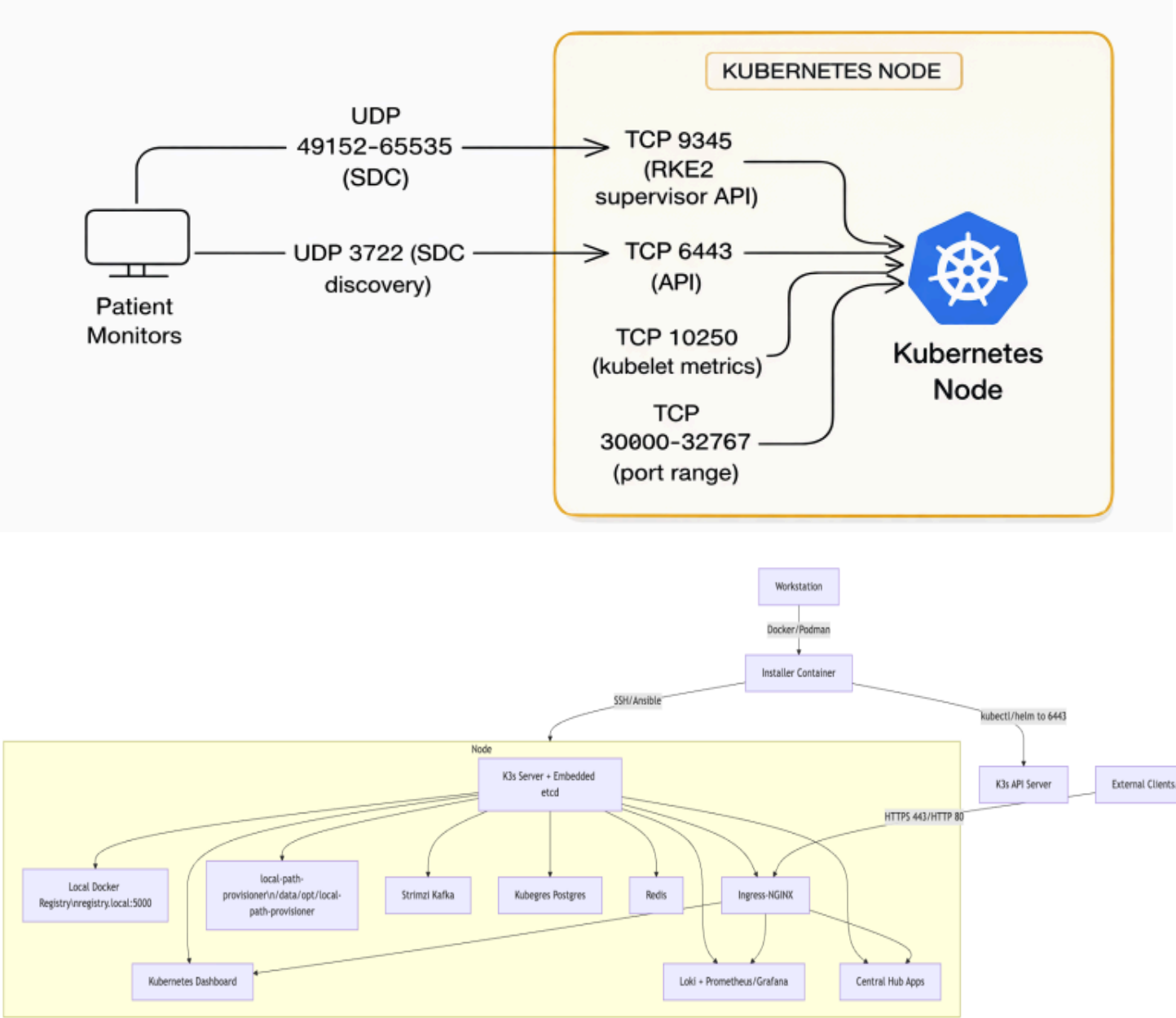
2.3.1 Konfiguration av nätverksport

Det centrala övervakningssystemet har följande konfiguration av portar. Observera att alla portar som inte används ska inaktiveras.

Tabell 5: Lista över konfiguration och beskrivning av nätverkets portar

Port	Källa	Destination	Beskrivning
53	Alla Kubernetes-noder	kube-dns / CoreDNS	DNS-upplösning
80	Diverse tjänster	autentisering, central övervakning, fleet-manager, kube-prometheus-stack-grafana	HTTP-tjänster
443	Diverse tjänster	Kubernetes-instrumentpanel, Kubernetes API, metrics-server, kube-prometheus-stack-operator	HTTPS/API-åtkomst
8080	Interna tjänster	hmdm-headwind-mdm, kube-prometheus-stack-alertmanager, kube-prometheus-stack-kube-state-metrics, kube-prometheus-stack-prometheus	Ändpunkter för interna tjänster
31000	MQTT-klient	hmdm-headwind-mdm	MQTT-kommunikation
5432	Apptjänster	postgres	Databasåtkomst
6379	Apptjänster	redis	Redis-kommunikation

Port	Källa	Destination	Beskrivning
8443	Metrikskrapa	kubegres-controller-manager-metrics-service	Metrik slutpunkt
9090	Övervakningsverktyg	kube-prometheus-stack-prometheus, prometheus-operated	Prometheus UI/API
9093	Hanterare av aviseringar	alertmanager-operated, kube-prometheus-stack-alertmanager	Alertmanager API
9094	Hanterare av aviseringar	alertmanager-operated, kube-prometheus-stack-grafana-headless	Cluster messaging (TCP)
9094	Hanterare av aviseringar	alertmanager-operated	Cluster messaging (UDP)
9100	Övervakningsagenter	kube-prometheus-stack-prometheus-node-exporter	Nodmetrik
9153	DNS-metrik	kube-dns, kube-prometheus-stack-coredns	CoreDNS-metrik
10250	Kubernetes-komponenter	kube-prometheus-stack-kubelet	Kubelet säker port
10255	Kubernetes-komponenter	kube-prometheus-stack-kubelet	Kubelet skrivskyddad port
4194	Metrikagent	kube-prometheus-stack-kubelet	cAdvisor-metrik
7946	Loki-tjänster	loki-medlemslista	Kommunikation om klustermedlemskap
3100	Loggningstjänster	loki, loki-headless	Loki-loggar
30080	Traefik	traefik NodePort (HTTP)	HTTP NodePort för ingång
30443	Traefik	traefik NodePort (HTTPS)	HTTPS NodePort för ingång



Figur 1: Diagram över klusternätverk för det centrala övervakningssystemet

Avsnitt 3. Instrumentpaneler och tjänster för administratörer

3.1 Kubernetes instrumentpanel

3.1.1 Åtkomst till Kubernetes instrumentpanel

Kubernetes instrumentpanel är tillgänglig via länken `https://dash.${your-domain-name}`.

För att komma åt instrumentpanelen måste man se till att DNS-posten finns för den här domänen hos sin DNS-leverantör.

Autentisering till instrumentpanelen kan göras med hjälp av `kubeconfig`-filen som genererades under installationen ELLER med hjälp av en token.

Se ”Allmän information om aktivering av det centrala övervakningssystemet” för information om hur man får tag på `kubeconfig`-filen.

Token kan hämtas från K8S-klustret med hjälp av kubectl-verktyget enligt följande:

För att komma åt instrumentpanelens token, följ dessa steg:

1. Leta reda på filen med namnet `dashboard-token.txt` efter att installationsprocessen har slutförts.
2. Den här filen finns i `creds`-mappen i installationsavbildningen.
3. Alla autentiseringsfiler, inklusive `dashboard-token.txt`, lagras i den här `creds`-mappen.

3.1.2 Användning av Kubernetes instrumentpanel

Det centrala övervakningssystemet innehåller en Kubernetes (K8s) instrumentpanel för att förbättra synligheten och hanteringen av det containeriserade centrala övervakningssystemet. Detta verktyg är avgörande för att upprätthålla kliniska systems operativa hälsa och efterlevnad, och ger viktiga insikter och kontroll över den infrastruktur som stöder verksamheten.

Viktiga funktioner och anpassningar:

- **Klusterhantering i realtid**: K8s instrumentpanel ger en översikt i realtid över klustrets hälsa, inklusive nodstatus, resursutnyttjande och prestanda för aktiverade applikationer. Det gör det möjligt för administratörer att effektivt övervaka och hantera Kubernetes-kluster som är värd för det centrala övervakningssystemet.
- **Hantering av arbetsbelastning**: Administratörer kan granska, hantera och felsöka arbetsbelastningar, inklusive aktiveringar, replikuppsättningar och poddar. Denna funktionalitet är avgörande för att säkerställa att kliniska applikationer fungerar smidigt och uppfyller de prestandakrav som krävs för säker och effektiv patientvård.
- **Övervakning av namnrymd**: Instrumentpanelen möjliggör övervakning av olika namnrymder och erbjuder en segmenterad vy av klustret som kan skräddarsys för specifika kliniska tillämpningar eller avdelningar inom vårdinrättningen.

- **Övervakning av resursutnyttjande**: Detaljerad metrik för användning av CPU, minne och lagring finns tillgängliga, vilket möjliggör proaktiv hantering av resurser för att förhindra prestandaförsämring som kan påverka den kliniska verksamheten.

3.1.3 Funktioner för IT-administratörer på sjukhus

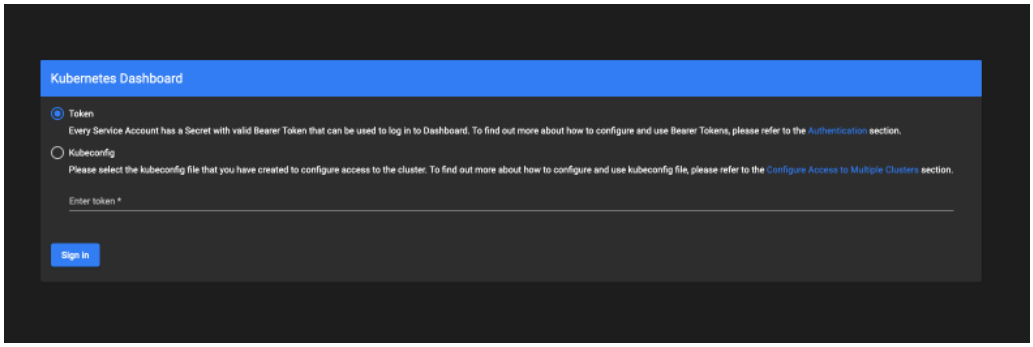
IT-administratörer på sjukhuset har befogenhet att:

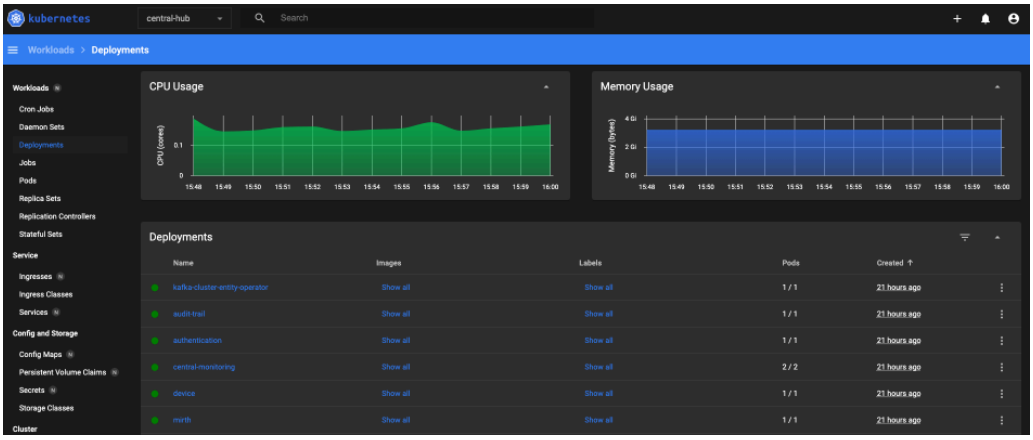
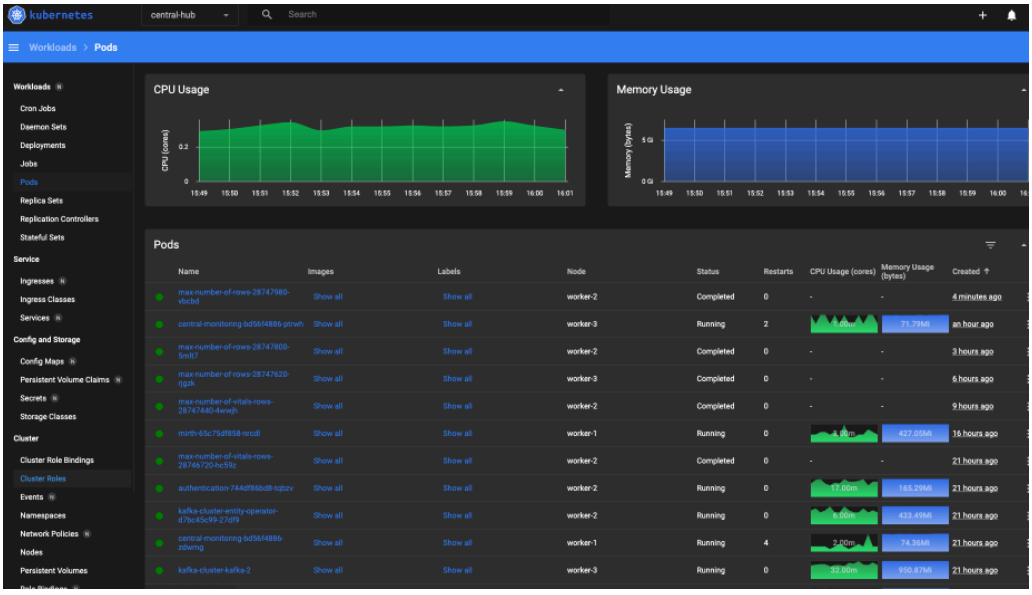
- **Aktivera och hantera applikationer**: Instrumentpanelen förenklar aktivering och hantering av applikationer inom Kubernetes-miljön. Administratörer kan uppdatera befintliga tjänster och hantera konfigurationer direkt via instrumentpanelen.
- **Övervaka klusterhändelser**: Instrumentpanelen tillhandahåller en omfattande logg över tjänster i det centrala övervakningssystemet, vilket gör det möjligt för administratörer att spåra ändringar, exportera loggarna och snabbt diagnostisera problem. Detta är avgörande för att upprätthålla efterlevnad och säkerställa att eventuella problem som påverkar det centrala övervakningssystemets tillämpningar omedelbart åtgärdas.
- **Hantering av resurskvoter**: Administratörer kan ställa in och tillämpa resurskvoter (skalning), vilket säkerställer att ingen enskild applikation eller användare förbrukar alltför stora resurser, vilket kan äventyra prestandan för andra kritiska kliniska applikationer.

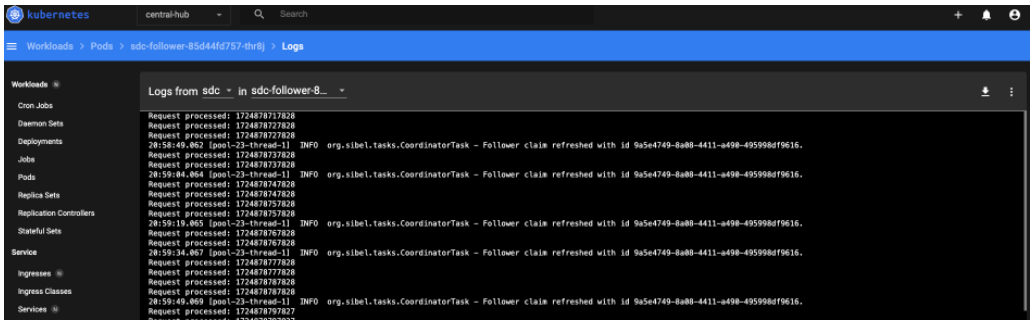
3.1.4 Övervakningsmetrik

- **Pod- och containerövervakning**: Kontinuerlig spårning av podstatus och containerhälsa för att säkerställa att alla komponenter i kliniska applikationer fungerar korrekt.
- **Noders hälsa och prestanda**: Övervakning i realtid av noders hälsa, inklusive CPU och minne, vilket säkerställer att infrastrukturen som stöder kliniska applikationer förblir robust och tillförlitlig.

Tabell 6: Kubernetes övervakningsmetrik

K8s instrumentpanel	**Bild**
Login	

Status för arbetsbelastning	
Aktiveringar	
Pods i drift	

Serviceloggar	

3.2 Grafana instrumentpanel

3.2.1 Åtkomst till Grafana instrumentpanel

Grafana instrumentpanel är tillgänglig via länken `https://mon.${your-domain-name}`.

För att komma åt instrumentpanelen måste man se till att DNS-posten finns för den här domänen hos sin DNS-leverantör. Vi rekommenderar att man använder domän med regex så att man inte behöver lägga till en specifik domän i sin DNS-leverantör (t.ex. *.{your-domain-name})

För att komma åt instrumentpanelens token, följ dessa steg:

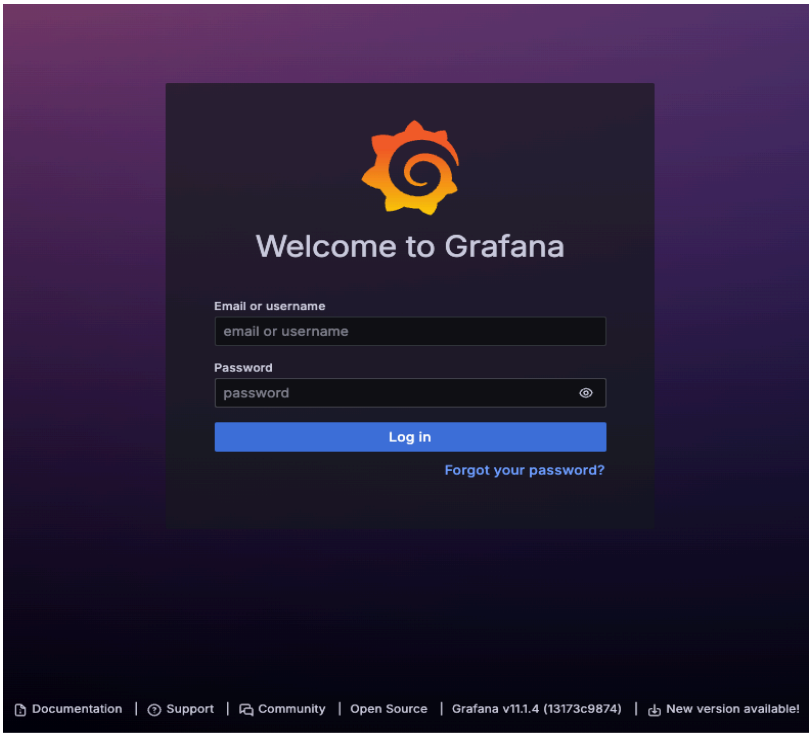
1. Leta reda på filen med namnet `monitoring.txt` efter att installationsprocessen har slutförts.
2. Den här filen finns i creds-mappen i installationsavbildningen.
3. Alla autentiseringsfiler, inklusive `monitoring.txt`, lagras i den här `creds`-mappen.

3.2.2 Användning av Grafana instrumentpanel

Det centrala övervakningssystemet för kliniska lösningar integrerar avancerade funktioner för händelsedetektering, loggning, aviseringar och övervakning, vilka är avgörande för att säkerställa tillförlitlighet och säkerhet i klinisk verksamhet, inklusive avvikelser i nätverket, inloggningsförsök eller ändringar i systemets konfiguration. Dessa funktioner möjliggörs via GPL-stacken – Grafana, Prometheus och Loki. Denna uppsättning verktyg för övervakning ger omfattande visualisering genom diagram, grafer och detaljerade logganalyser, vilka täcker alla komponenter i det centrala övervakningssystemet, inklusive tjänster i det centrala övervakningssystemet, infrastrukturtjänster, servertrafik och nätverksövervakning.

Viktiga funktioner och anpassningar:

- **Fördefinierade instrumentpaneler och anpassning**: Som standard är systemet utrustat med 20+ fördefinierade instrumentpaneler som ombesörjda av Sibel-teamet. Dessa instrumentpaneler erbjuder omfattande insikter i olika parametrar för driften. Dessutom stöder övervakningsplattformen fullständig anpassning av instrumentpaneler och aviseringsregler för att möta specifika kliniska behov.
- **Lagring av loggar**: För att optimera lagring och prestanda är standardperioden för lagring av loggfiler inställd på 7 dagar. Denna period är utformad med hänsyn till balansen mellan lagringskapacitet och behovet av historiska data i kliniska miljöer.
- **Inloggning**



Figur 2: Versionen av Grafana ska verifieras från inloggningsfönstret

3.2.2.1 Funktioner för IT-administratörer

IT-administratörer har befogenhet att:

- **Skapa anpassade instrumentpaneler och aviseringar**: Administratörer kan utforma instrumentpaneler som är skräddarsydda efter deras operativa krav och ställa in anpassade aviseringar för att säkerställa proaktiv övervakning.
- **Hantering av användare**: Systemet stöder rollbaserad åtkomstkontroll (RBAC), vilket gör det möjligt för administratörer att skapa och hantera användare med lämpliga åtkomstnivåer, vilket säkerställer säker drift som efterlever regelmässiga krav.

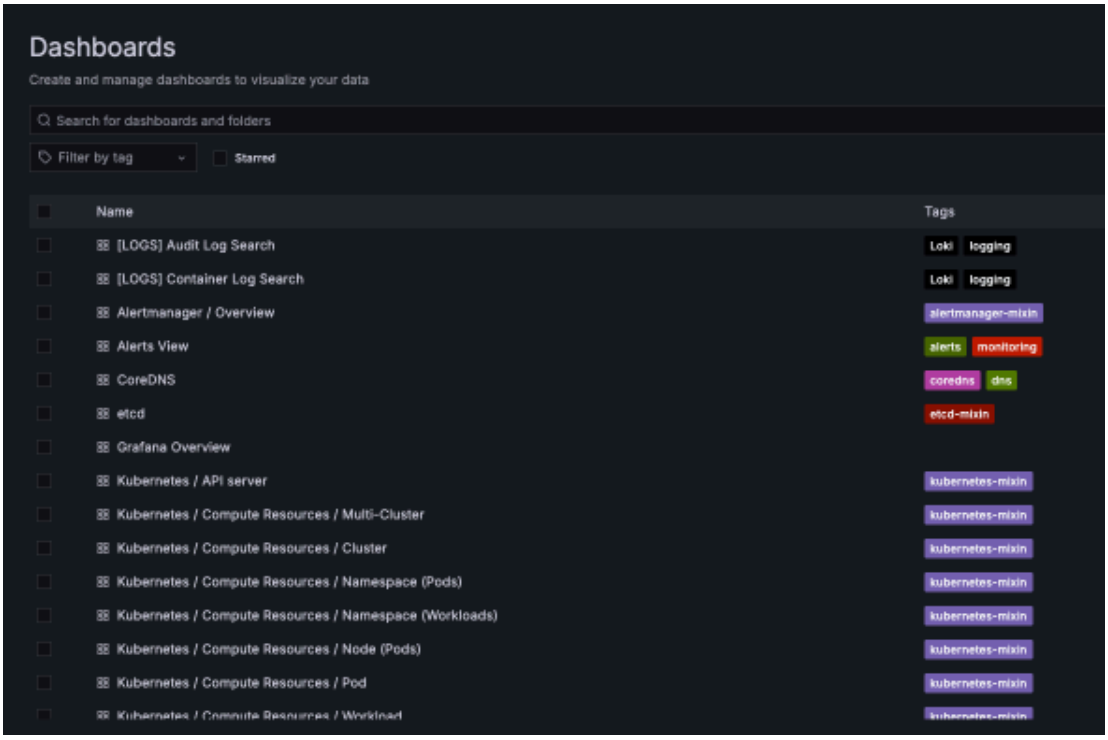
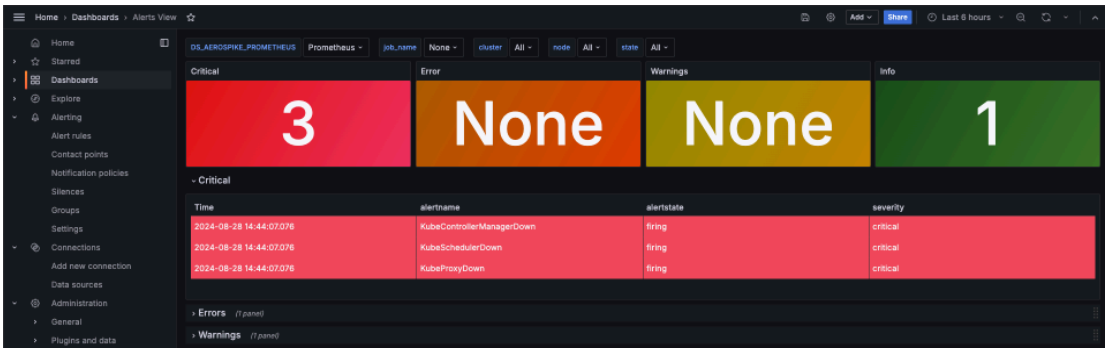
3.2.2.2 Övervakningsmetrik

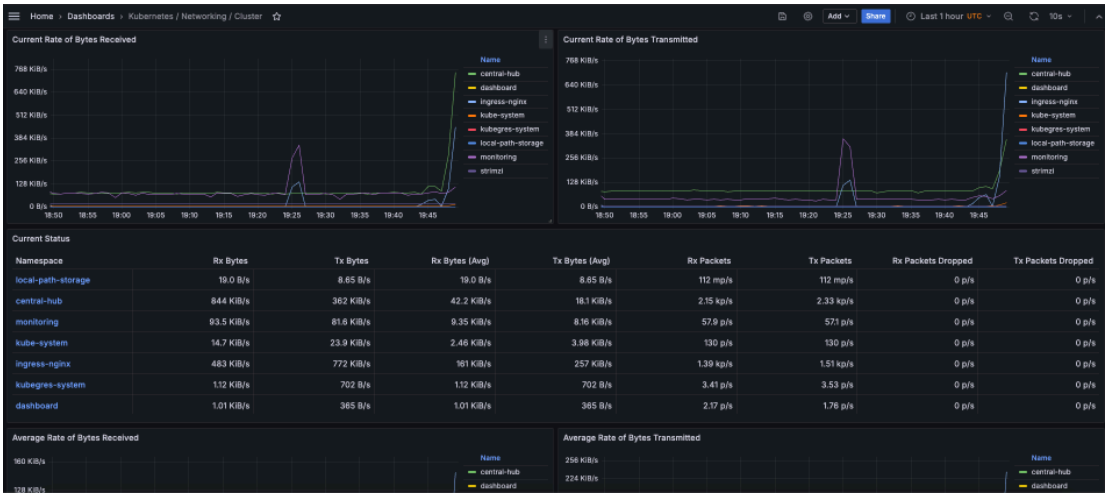
Övervakningsverktyget erbjuder detaljerad metrik och loggar, inklusive:

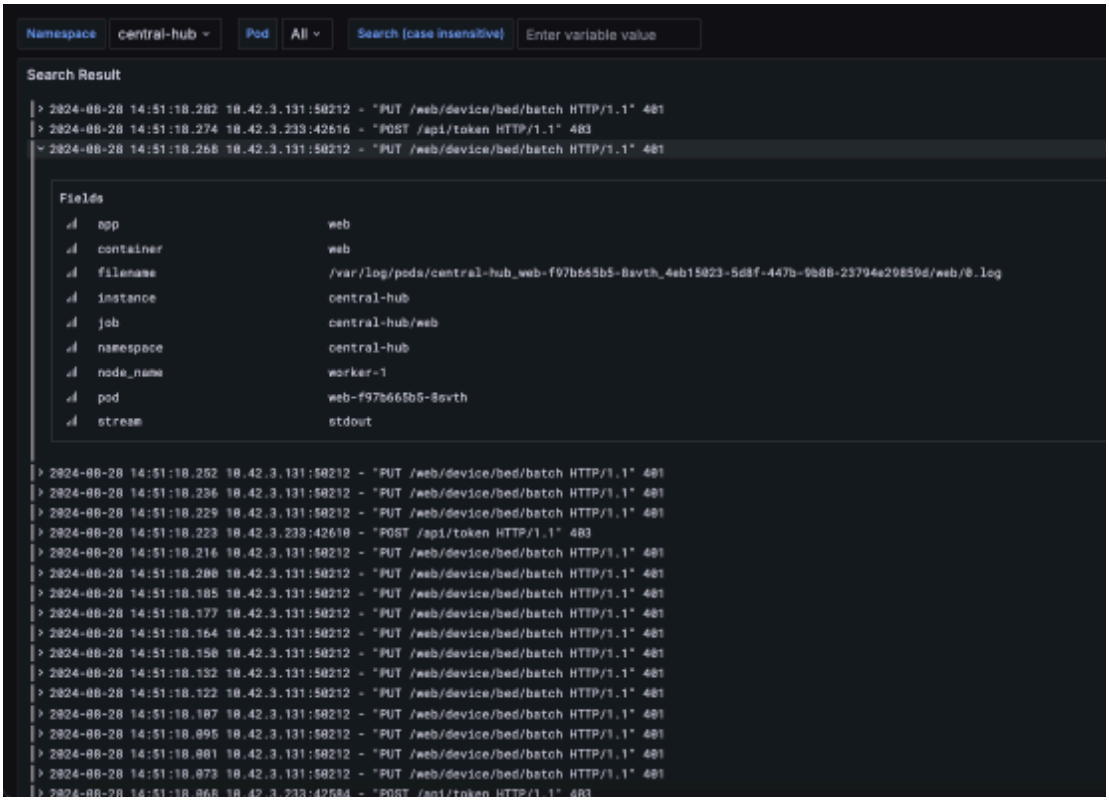
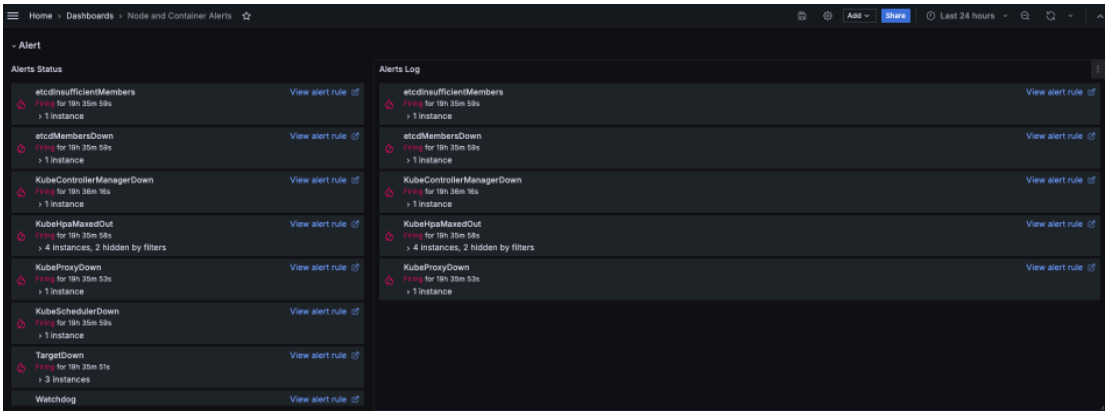
- **Statistik över servertillgänglighet**: Kontinuerlig uppföljning av serverns drifttid och tillgänglighet för att säkerställa systemets tillförlitlighet.
- Sökning i containerloggar: Effektiva sökfunktioner i containerloggar för snabb felsökning och analys.
- **Övervakning av resursutnyttjande**: Realtidsövervakning av användning av CPU, minne och diskar i hela systemet.
- **Kluster- och nodövervakning**: Omfattande insikter i klusterresurser, nodprestanda och övergripande systemhälsa.
- **Övervakning av nätverkets arbetsbelastning**: Detaljerad övervakning av trafik på nätverket för att förhindra flaskhalsar och säkerställa optimala prestanda.
- **Revisions- och proxyloggar**: Underhåll av detaljerade revisionsloggar och proxyloggar för att stödja efterlevnad av kliniska och regulatoriska standarder.

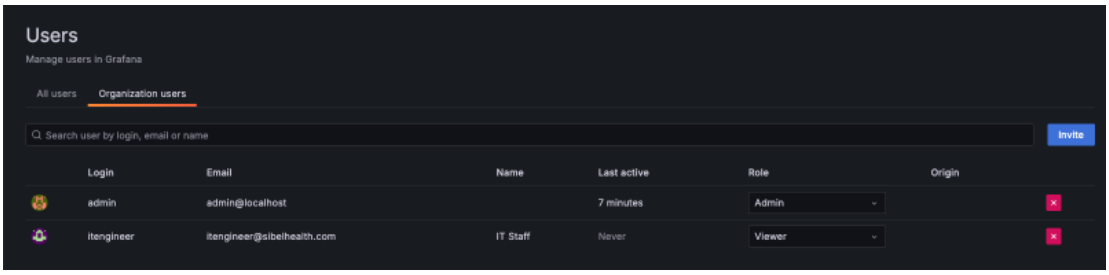
- **Loggning av konsumentintegration**: Systemet integreras med kompatibla system för detektering av intrång (IDS) och lösningar för hantering säkerhetsinformation och händelser (SIEM).

Tabell 7: Grafana övervakningsmetrik

Grafana	**Bild**
Instrumentpanel	
Aviseringsvy	

Klusterresurs	
Nätverkande	

Containerloggar	
VM-resurs	
Nod- och tjänsteaviseringar	

Skapande och hantering av användare (RBAC)	

Denna övervakningslösning är utformad för att säkerställa säker, effektiv och kompatibel drift av centrala övervakningssystem, i linje med FDA:s riktlinjer för medicinsk programvara.

3.2.3 Lagring av loggar

Systemet lagrar loggar i obearbetat (rått) format och JSON-format:

- Obearbetade (råa) loggar är formaterade som följer:

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

- Loggarna för balansering av belastning är JSON-formaterade:

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

De administrativa agenterna i Kubernetes-klustret dirigerar containerkörningen att skriva loggarna på applikationsnivå till katalogen, `/var/log/pods`. Dessutom lagras Kubernetes-klustrets loggar för systemnivå inom `/var/lib/rancher/rke2/server/logs`.

Loggarna roteras här baserat på tillgängligt diskutrymme. Standardkonfigurationen för rotation är:

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

Logginsamlingsagenten, Promtail, tar in applikationsloggarna i `/var/log/pods` från var och en av loggarna för Kubernetes-noder och systemnivå i `/var/lib/rancher/rke2/server/logs` från kontrollplanets noder och pushas sedan till Loki som fungerar som en databas för loggar.

Loggarna för nätverksnivå från den virtuella lastbalanseraren VM, lagras i `/var/lib/docker/containers/`-katalogen med Promtail-agenten som kör jämsides, och pushas sedan till Loki.

3.2.4 Hantering av enhetshändelser

När avvikande förhållanden upptäcks reagerar systemet därefter. Om till exempel kontinuerliga inloggningsförsök identifieras, till exempel fem felaktiga försök i rad till inloggning, blockerar systemet ytterligare inloggningsförsök i 15 minuter.

Alla okända enheter utan giltiga certifikat svartlistas och nekas kommunikation med systemet. Om alltför kraftig trafik på nätverket upptäcks, vilket påverkar normal verksamhet, stoppar systemet dessutom dataströmningen och aviserar slutanvändare om nätverksproblemet via felmeddelanden. ANNE View-sessionen mellan sensorerna och ANNE View påverkas inte. Dessa avvikelser övervakas i realtid och loggas med hjälp av det centrala övervakningssystemets lösning för övervakning.

3.3 Lokal MDM instrumentpanel

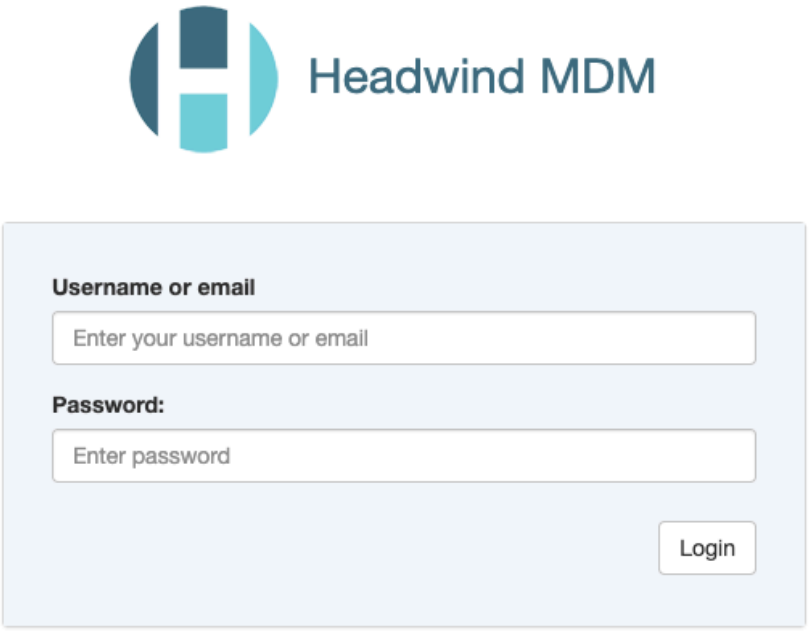
Den lokala MDM instrumentpanelen är tillgänglig via länken `https://hmdm.${your-domain-name}`.

För att komma åt instrumentpanelens gränssnitt, se till att följande konfiguration är på plats: En DNS-post måste ha skapats för den angivna domänen via DNS-leverantören. Utan detta tolkas inte instrumentpanelens URL korrekt.

Autentisering:

- Använd den tilldelade e-postadressen för teknisk användare som användarnamn.
- Standardlösenordet är: 'admin'.

Vid första lyckade inloggning uppmanar systemet användaren att **skapa ett nytt lösenord**. Detta är ett obligatoriskt steg för att fortsätta med vidare åtkomst.



Figur 3: Lokalt gränssnitt för inloggning i MDM instrumentpanel

3.3.1 MDM-licens och enhetsregistrering

För att få tillgång till MDM-systemets fulla funktionalitet, se till att IT-administratören har en giltig licensnyckel. Denna licensnyckel måste tillämpas efter att CMS-installationen är klar och levererad av tillverkaren.

Enhetsregistrering och konfiguration:

IT-administratören kan med hjälp av det lokala MDM-gränssnittet:

- Registrera ANNE Views med hjälp av konfigurationsinställningarna från Sibel Health.
- Installera appen Anne-View på registrerade enheter.
- Aktivera och konfigurera Kiosk Mode för att säkerställa att enheten är låst i den avsedda kliniska användningsmiljön.

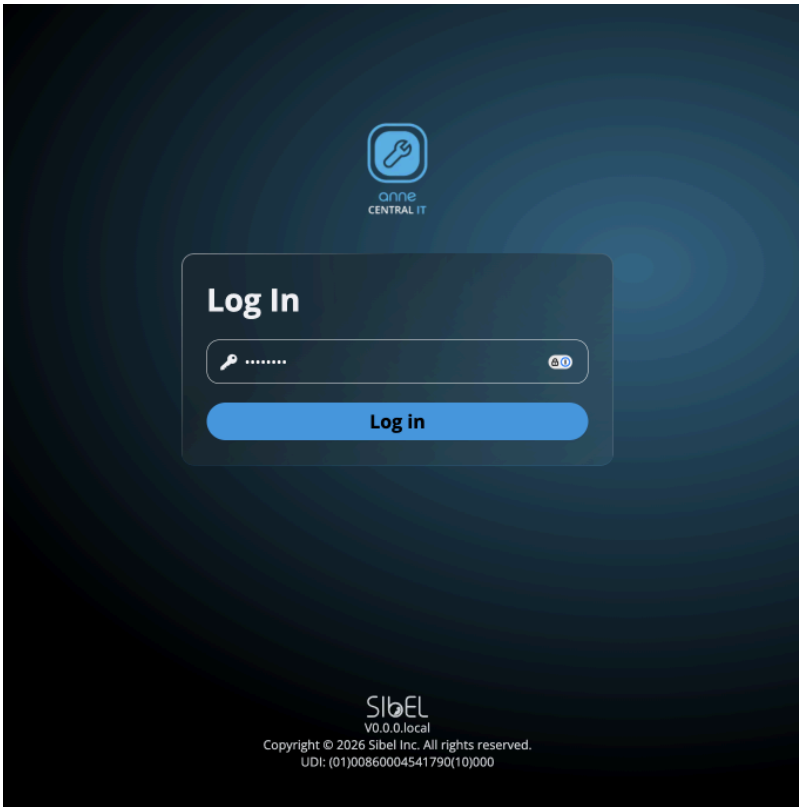
Korrekt licensiering och inställning efter installation krävs för att säkerställa säker och stabil hantering av enheter.

3.4 Adminhubb

3.4.1 Inloggning

Adminhubben är tillgänglig via länken `https://cms.${your-domain-name}`.

Ange ditt lösenord för att logga in på centralhubben. Och klicka på knappen ”Log in”.



Obs: IT-administratören konfigurerar kontot och lösenordet under installationen.

3.4.2 Felhantering

Tabell 8: Hantering av inloggningsfel i adminhubben

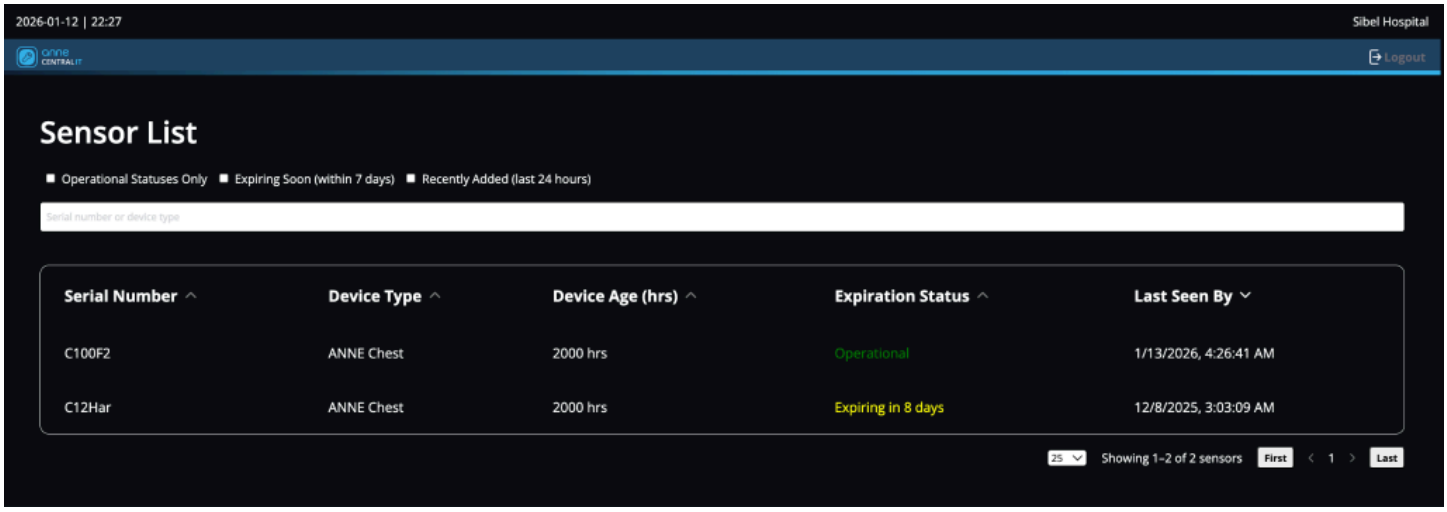
Felmeddelande	Grundorsak	Användarens rekommenderade åtgärd
Serverfel Försök igen om några minuter.	Serverfel i systemet.	Försök igen senare eller kontrollera tjänstens status. Om problemet kvarstår, kontakta Sibel Healths support.
Felaktigt lösenord. Försök igen.	Användaren anger fel lösenord.	Försök igen med rätt lösenord.
För många försök. Försök igen om 15 minuter.	Användaren misslyckades med att ange lösenordet minst 5 gånger.	Försök igen efter 15 minuter. Återställ lösenordet om det är glömt.

3.4.3 Instrumentpanel för sensors livstid

Efter lyckad inloggning kan IT-administratören:

- Visa lista över enheter som är registrerade i CMS.
- Adminhubben visar information som serienummer, enhetstyp, enhetens ålder, utgångsstatus och tidsstämpel för senast sedd.
- Följande filter stöds för användarens bekvämlighet: Driftstatus, Utgångsstatus inom 7 dagar, Nyligen tillagd under de senaste 24 timmarna, Serienummer och Enhetstyp.
- Enhetens ålder och utgångsdatum kan vara otillgängligt för enheter som inte är tillverkade av Sibel, patientmonitorer och OEM-enheter.

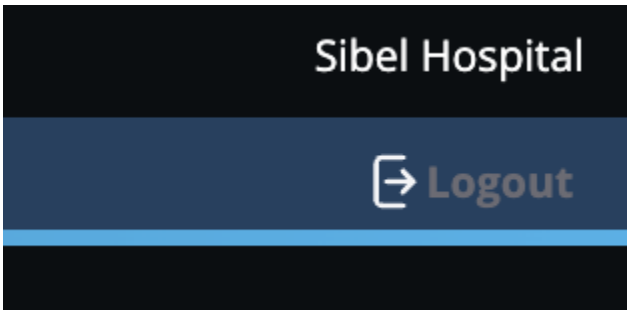
Obs: Patientmonitorer och sensorer kallas här gemensamt för enheten.



Figur 4: Instrumentpanel för sensors livstid

3.4.4 Logga ut

Klicka på knappen ”Logout” i det övre högra hörnet.



Obs: IT-administratören loggas automatiskt ut efter 15 minuters inaktivitet.

Avsnitt 4. Underhåll av centralt övervakningssystem

4.1 Underhåll av centralt övervakningssystem

4.1.1 Överväganden gällande cybersäkerhet för det centrala övervakningssystemet

Sibel Health har följande övervägande gällande säkerhet för installationen av ANNE View och det centrala övervakningssystemet för att ge högsta möjliga säkerhetsnivå.

- Autentisering mellan ANNE View och den centrala servern använder X.509 certifikatkedja baserad på certifikat och valideringskedja; endast inkommande förfrågningar från ANNE View valideras av den centrala servern. Rekommenderad certifikatgenerering är att använda 1 års utgångsdatum, med hjälp av openssl med RSA:4096 kryptering.
- Inga PHI-data lagras i det centrala övervakningssystemets databas.
- JSON Web Token används för säker dataöverföring mellan det centrala övervakningssystemets webbportal och backend-gatewayen. Access-token är giltig i 15 minuter och refreshtoken är giltig i 7 dagar.
- Det centrala övervakningssystemet använder inte en huvuddatabas för lagring av nycklar för att undvika risken för brute force-attacker, osäker lagring och attacker på sidokanaler.
- Sibel Health rekommenderar att certifikatens giltighetstid sträcker sig från minst 6 månader till högst 1 år, för att säkerställa en balans mellan säkerhet och effektivitet.

4.1.2 Säkerhetspatchningar för det centrala övervakningssystemet

Explicita patchar som riktar sig mot upptäckta sårbarheter är obligatoriska patchar och bör uppdateras så snart de tas emot. Dessa säkerhetsrelaterade patchar kommer inte att innehålla ny funktionalitet och ska vara fristående patchar som aktiveras för att säkra produkten från sårbarheten.

När en patch är fullständig och godkänd distribuerar Sibel Health patchen till klienterna via ett säkert, hårdvarukrypterat USB-minne.

Säkerhetspatchningar för det centrala övervakningssystemet kan installeras av en IT-administratör med åtkomst till det centrala övervakningssystemets installation. Stegen för tillämpning av säkerhetspatchningar för det centrala övervakningssystemet är desamma som det centrala övervakningssystemets uppgraderingssteg som nämns i avsnitt 5 (sidan 35) av SDD-SW-031-007 installationsmanualen för det centrala övervakningssystemet.

Man kan verifiera den senaste versionen med hjälp av K8s instrumentpanel genom att kontrollera avbildningsversionen.

4.1.3 Patchningar för centrala övervakningssystem

Hastigheten för patchning av det centrala övervakningssystemet följer en tvåveckors sprintcykel och snabbkorrigeringsprocess. Sibel Health distribuerar patchar.

4.1.4 Releaser av det centrala övervakningssystemets versioner

Fullständiga versioner av det centrala övervakningssystemet genereras baserat på Sibel Healths interna livscykel för utvecklingar. Förfarandet för att releasa versioner följer lämpliga testfaser (verifiering och validering) för att producera en release med ny funktionalitet och korrigeringar av avvikelser från tidigare versioner såväl som prestandaförbättringar. Distribution av releaser sker genom Sibel Health.

4.1.5 Säkerhetskopiering och återställning av det centrala övervakningssystemet

Vid aktiveringen av det centrala övervakningssystemet måste säkerhetskopior av databasen aktiveras. Denna installation inkluderar inte integration med extern datalagring, och därför stöds inte automatisk säkerhetskopiering av data. Det krävs att databasen säkerhetskopieras manuellt varje vecka som ett förfarande för återställningar i händelse av katastrofala tillbud.

Säkerhetskopiorna ska lagras både på plats och på extern plats för att säkerställa dataredundans och säkerhet. Säkerhetskopiering ska schemaläggas under timmar med låg trafik för att minimera påverkan på den operativa verksamheten. Regelbunden övervakning är avgörande för att validera säkerhetskopiornas integritet och tillförlitlighet.

I händelse av kritiska funktionsfel finns detaljerade instruktioner för säkerhetskopiering/återställning i avsnitt 3.1.3 (sidan 28) av SDD-SW-031-007 i det centrala övervakningssystemets installationsmanual. Kritiska funktioner som de ovan kan inte konfigureras av obehöriga användare, liksom beskrivningen av tillåtna kommunikationsportar i avsnitt 4.1.

Det centrala övervakningssystemet består av ett antal virtuella maskiner som kör Kubernetes-klustret. Klusternoderna lagrar på obestämd tid en bild av konfigurationen för var och en av noderna i klustret. Som del av den automatiska återställningsmekanismen körs tjänsterna i det centrala övervakningssystemet som poddar på arbetsnoderna. Om någon tjänst (podd) går förlorad skapar klustrets failover- och återställningsmekanismer automatiskt en ersättningspodd med samma ursprungliga konfiguration, varpå klustret återställs till full kapacitet och funktionalitet.

Om ett fall uppstår som kräver en manuell återställning av en konfigurationsfil kan en autentiserad och auktoriserad administratör kopiera konfigurationen från en annan nod för att återställa klustret till full kapacitet och funktionalitet.

4.1.6 Loggning av händelser i det centrala övervakningssystemet

Sibel Health tillhandahåller funktioner för loggning och övervakning av verifieringskedjor inom sina system och delsystem. Dessa loggar och metriker informerar om systemens hälsa och prestanda såväl som avvikelser och problem inom systemens komponenter. Dessa händelser kommer att vara en administrativ funktion och tillgängliga i administratörens instrumentpanel för att kontrollera status, loggar, metriker och diagram.

Sjukhusets IT-administratörer måste regelbundet granska loggarna genom ett standardiserat förfarande för kontinuerlig övervakning.

4.1.7 Det centrala övervakningssystemets kryptografiska kontroll

Sibel Health ska hantera livscykeln för nycklar och certifikat via lämpliga kryptografiska moduler såsom 1Password; dessa moduler tillhandahåller kryptering, åtkomstkontroll och säker lagring av känsliga data. Alla kryptografiska tillgångar hanteras och underhållas av Sibels chef för informationssäkerhet, i enlighet med rekommendationerna i NIST SP 800-131A, Transitioning the Use of Cryptographic Algorithms and Key Lengths och FIPS 140-3, Security Requirements for Cryptographic Modules.

4.1.7.1 Lagring av kryptografiska tillgångar

Sibel Health lagrar och underhåller kryptografiska tillgångar, nycklar och certifikat i 1Passwords säkra valv genom att använda avancerade krypteringsalgoritmer för att förhindra obehörig åtkomst och genom att säkerställa

kontrollerad åtkomst endast för behörig personal. 1Password säkerställer krypterad säkerhetskopiering av lagrade tillgångar för att stödja failover-mekanismen.

I de fall där klienter begär kontroll över kryptografiska tillgångar på grund av deras organisationers interna krav på cybersäkerhet, informerar Sibel Health klienterna om att man tillämpar passande kryptografiska moduler i enlighet med bästa praxis för cybersäkerhet, såsom FIPS 140-3, Security Requirements for Cryptographic Modules.

- FIPS 140-3 (FIPS 140-2 avsnitt 4.7) beskriver krav gällande hantering av kryptografiska nycklar.

4.1.7.2 Åtkomstkontroll för kryptografiska tillgångar

Alla kryptografiska tillgångar ska krypteras och åtkomsten strikt kontrolleras genom en policy för rollbaserad åtkomstkontroll (RBAC) av Sibels utsedda IT-/säkerhetschef; Sibel Health följer den policy för åtkomstkontroll som rekommenderas av FIPS 140-3.

Sibel Health förser också sina klienter med rekommendationer för hur de ska utforma policy för sin åtkomstkontroll enligt detta. Rekommendationerna från Sibel Health beaktar rollerna och tjänsterna:

- IT-administratör (superuser)
    - Fungerar som superuser, styr policy för åtkomstkontroll och hanterar livscykeln för kryptografiska tillgångar.
- Vårdpersonal (användare)
    - Fungerar som användare med tillgång till de kliniska lösenorden för det centrala övervakningssystemet.

4.1.7.3 Generering och förnyelse av kryptografiska tillgångar (rotation)

Kryptografiska nycklar och certifikat genereras före och under aktiveringen av det centrala övervakningssystemet.

Nycklarna och certifikaten som krävs före aktivering är:

- Digitala nyckelpar för signaturer till programvaran för både ANNE View och det centrala övervakningssystemet
- Certifikatkedjan till TLS/SSL för säker nätverkskommunikation inom det centrala övervakningssystemet
- Sibels certifikatkedja till rootCA och IntermediateCA för säker autentisering och kommunikation mellan ANNE View och det centrala övervakningssystemet

På klientens begäran gällande sin egen kryptografiska hantering förser Sibel Health klientens IT-administratör med följande information:

- Kryptografiska algoritmer och protokoll
- Kryptografisk giltighet

När kryptografins giltighetstid närmar sig slutet förnyar eller roterar Sibel Health nycklarna och certifikaten i enlighet med NIST SP 800-57 del 1, Recommendation for Key Management, och NIST 1800-16B, Securing Web Transactions.

Sibel Health spårar nycklar och certifikats giltighet via den kryptografiska modulen 1Password som konfigureras för att meddela Sibel Healths IT-/säkerhetschef eller ingenjör för cybersäkerhet 30 dagar före rotation av nycklar eller förnyelse av certifikat.

Klientens IT-administratörer rekommenderas att utföra nyckelrotationen av det centrala övervakningssystemets programvara enligt de kryptoperioder som beskrivs i tabell 9.

Tabell 9: Rekommenderade kryptoperioder och giltighet för certifikat per tillgångstyp enligt NIST SP 800-57 del 1 och NIST SP 1800-16B

Tillgångens namn	Tillgångens typ	Giltighet / Kryptoperiod
Nyckel		
Digital signatur	Privat nyckel för signatur	1 till 3 år
Digital signatur	Offentlig nyckel för verifiering av signatur	Inte specificerad, men följer privat nyckel (1 till 3 år)
Autentisering av användare	Privat nyckel för autentisering	1 till 2 år
Autentisering av användare	Offentlig nyckel för autentisering	1 till 2 år
Postgres krypteringsnyckel	Nycklar för symmetrisk datakryptering	3 år
Lösenord		
Postgres autentiseringsnyckel	Lösenord	1 år
Redis autentiseringsnyckel		
Administrativt lösenord		
Token för administrativ instrumentbräda		
Lösenord för övervakningspanelen		
Certifikat		
TLS/SSL-certifikat	Certifikat	1 år
IntermediateCA-certifikat		

Att upprätthålla säker kommunikation och kryptografi inom systemet kräver snabb förnyelse av certifikat och nyckelrotation. Certifikat ska förnyas och valideras minst 30 dagar innan det nuvarande certifikatet löper ut, och nycklarna ska roteras enligt kryptoperioden. Sibel Health följer NIST SP 1800-16B:s riktlinjer för förnyelse av certifikat.

Följande steg beskriver processen för att förnya certifikat och leverera dem till klienter:

- **Övervaka certifikatets utgångsdatum**: Sibel Healths IT-/säkerhetsteam kontrollerar varje månad certifikatets utgångsdatum via den kryptografisk modulen 1Password. Sibel Health ska kräva att klientens IT-administratörer i god tid kontrollerar certifikatets utgångsdatum i de fall att de själva hanterar certifikaten.
- **Generera begäran om certifikatsignering (CSR)**: Skapa en ny CSR för certifikatförnyelsen. Använd befintliga privata nycklar eller generera nya för att få ett nytt certifikat.
- **Skicka in CSR till certifieringsmyndighet (CA)**: Skicka in CSR till en betrodd CA.
- **Erhåll nytt certifikat**: Ta emot den nya uppsättningen certifikat när valideringen är fullbordad.
- **Leverans av nytt certifikat**: Sibel Healths IT-/säkerhetsteam delar förnyade certifikat med klienters IT-administratörer via 1Password.
- **Certifikatbyte**: Sibel Healths IT-/säkerhetsteam kommunicerar med klientens IT-administratörer strikt i enlighet med avsnitt 4.5 (sidan 34) av SDD-SW-031-007 installationsmanual för det centrala övervakningssystemet för att uppnå lyckade byten av certifikat.
- **Installera certifikatet**: Installera/ersätt det nya certifikatet i det centrala övervakningssystemet.
- **Starta om tjänster**: Starta om tjänsterna i det centrala övervakningssystemet för att tillämpa det uppdaterade certifikatet.

- **Verifiera systemets funktionalitet**: Kontrollera det centrala övervakningssystemet för att säkerställa att de nya certifikaten fungerar korrekt.

Det är också avgörande för sjukhusets IT-administratörer att nyckelrotationen av det centrala övervakningssystemets programvara utförs enligt instruktionerna i avsnitt 4.4 (sidan 31) av SDD-SW-031-007 installationsmanual för det centrala övervakningssystemet. Sibel Health meddelar klienterna när nyckelrotation ska ske, baserat på systeminstallationens tidslinje och via säker e-postkommunikation.

När nycklarna eller certifikaten har ersatts eller roterats till systemet ska sjukhusets IT-administratörer bekräfta det centrala övervakningssystemets funktionalitet och verksamhet.

För att säkerställa att det centrala övervakningssystemet fungerar korrekt:

- **Administratörs instrumentpanel validering av IT-administrering**: Sjukhusets IT-administratörer kan verifiera infrastrukturens funktionalitet via administratörens instrumentpanel för att säkerställa att alla tjänster är fungerande. Ett övervakningsverktyg som är installerat för att stödja detektering av händelser kan också användas för validering.
- **Administratörs instrumentpanel för valdering**: Sjukhusets IT-administratörer kan verifiera systemets grundläggande funktioner genom att kontrollera användares behörighet och säkerställa att systemet utför sin avsedda funktion korrekt.

4.1.7.4 Återkallelse av kryptografiska tillgångar

I fall av att nyckel/certifikat blivit komprometterade,

- återkallelse av nyckel
- återutgivning
- omkonfiguration

I händelse av att det upptäcks att en nyckel eller ett certifikat komprometterats eller att utgångsdatumet har passerats eller krypteringsperioden löpt ut, ska Sibel Healths IT-/säkerhetsteam vidta omedelbara åtgärder, inklusive återkallelse av nycklar, återutgivning och omkonfigurering av berörda system, och även uppmana kunder att vidta omedelbara åtgärder för att minska säkerhetsriskerna.

Förfarandet ska följas som beskrivs i avsnitt 4.1.7.3, Generering och förnyelse av kryptografiska tillgångar (rotation):

- Generering av kryptografi
- Återkallelse av nyckel
- Återutgivning av kryptografi
- Ersättning
- Verifiering av funktion

4.1.7.5 Radering/förstörelse av kryptografiska tillgångar

Sibel Healths IT-/säkerhetschef ska för de kryptografiska nycklar och certifikat som inte längre används förstöra oanvända kryptografiska tillgångar och oåterkalleligt radera dem från den kryptografiska modulen. Detta förhindrar alla möjligheter att återställa eller rekonstruera kryptografiska nycklar eller känsliga uppgifter. Sibel Health följer riktlinjerna i NIST SP 800-88, som tillhandahåller standarder för säker datasanering.

Sibel Healths IT-/säkerhetschef ska bekräfta att klientens IT-administratörer följer samma protokoll för att säkerställa nollställning av kryptografiska tillgångar.

4.2 Avveckling av det centrala övervakningssystemet (EOL)

4.2.1 Versionen av det centrala övervakningssystemet stöds inte längre

Versionerna av det centrala övervakningssystemet kommer att stödjas upp till två versioner bakåt, men när en version inte längre stöds instrueras klienter om hur man uppgraderar till den senaste versionen. Användare som väljer bort uppgraderingar erhåller inte längre några uppdateringar (säkerhet eller patchar). Sibel Health tar fram information åt klienterna om kända sårbarheter för att informera dem om riskerna med att inte gå över till den senaste versionen.

4.2.2 Det centrala övervakningssystemet uttjänt

När det centrala övervakningssystemet når slutet på sin livscykel informerar Sibel Health alla klienter om det datum då det inte längre finns något stöd för systemet och man inte längre kan förvänta sig att det är tillförlitligt. Sibel Health har skapat ett dokument, SDD-SW-031-007 installationsmanual för det centrala övervakningssystemet, inklusive avvecklingsprocedurer i avsnitt 6 (sidan 37) för att säkert ta bort applikationen från dess installerade plats såväl som ger alternativ för radering av data.

Observera att känslig information kan exponeras om systemet tas ur drift felaktigt eller ofullständigt:

- För- och efternamn
- Födelsedatum
- Patient-ID

Avsnitt 5. Felsökning

5.1 Validering av anslutning till 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
```

Om detta felmeddelande visas:

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

Det betyder att konfigurationsfilen saknas på sin standardplats `~/.kube`. Se till att filen kopieras från installationsplatsen till standardplatsen och försök igen. Filen ska vara exakt konfigurerad och finnas i katalogen för `~/.kube`.

För att förenkla kommunikationen med Kubernetes klusterfil ka ‘~/sibel-install/kubeconfig’ kopieras till ‘~/.kube’-katalogen med namnet config vilket är en plats som kubectl kontrollerar och använder som standard.

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

Filen `~/.kube/config` ska se ut ungefär så här:

```
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 Fel vid installation av det centrala övervakningssystemet

Under installationsprocessen kan man stöta på följande eller liknande fel:

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

I de flesta fall betyder det att man har hoppat över installationsmanualens steg för att skapa DNS-poster. DNS-posterna krävs för att komponenterna i det centrala övervakningssystemet ska kunna kommunicera med varandra. DNS-posterna ska skapas i DNS-leverantören för den domän som används för aktiveringen av det centrala övervakningssystemet och även för Kubernetes API-domän.

DNS-posterna ska skapas för följande domäner:

```
- 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 lösning för Kubernetes API-domän kan man lägga till följande rad i `/etc/hosts`-filen på maskinen där installationen körs:

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

5.3 Fel på det centrala övervakningssystemets tjänster

Om det centrala övervakningssystemet inte fungerar som förväntat kan följande steg vidtas för att felsöka problemet:

1. Kontrollera statusen för komponenterna i det centrala övervakningssystemet med följande 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
```

Man kan alternativt göra detta med användning av Kubernetes instrumentpanel. Logga in på instrumentpanelen och navigera till namnrymnden för `central-hub` och kontrollera statusen för poddarna på `Workloads`-sidan.

2. I de fall att det skulle finnas poddar som inte är `Running` eller `Completed` , kontrollera deras loggar för att identifiera problemet. Loggarna kan kontrolleras med följande kommando:

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

Eller använd Kubernetes instrumentpanel. Navigera till namnrymnden för `central-hub` och kontrollera poddens loggar på `Workloads`-sidan.

3. Om några av poddarna är i tillståndet `Pending`, kontrollera händelserna i poden för att identifiera problemet. Händelserna kan kontrolleras med följande kommando:

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

Eller använd Kubernetes instrumentpanel. Navigera till namnrymnden för `central-hub` och kontrollera poddens händelser på `Workloads`-sidan.

Händelser är vanligtvis självförklarande och kan hjälpa till att identifiera problemet.

En möjlig orsak till att poddar hänger som ”pending” kan vara att noden där podden ska schemaläggas inte är redo eller att det inte finns tillräckligt med resurser på noden för att schemalägga podden.

Nodens status kan kontrolleras med följande 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
```

Kontrollera om en av noderna inte är `Ready` nodens händelser och tillstånd för att identifiera problemet med följande kommando:

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

Läs utdata noggrant för att identifiera eventuella problem med noden.

5.4 URL för det centrala övervakningssystemet inte tillgänglig

Om det centrala övervakningssystemets URL inte är tillgängligt kan följande steg vidtas för att felsöka problemet:

1. Se till att DNS-posten finns hos DNS-leverantören för det centrala övervakningssystemets URL. Den korrekta IP-adressen är IP-adressen för lastbalanseraren som skapades under installationsprocessen.

2. Om DNS-posten finns är nästa steg att kontrollera om ingångskontrollen i Kubernetes-klustret fungerar korrekt. Ingångskontrollen ansvarar för att dirigera trafiken till rätt tjänst i Kubernetes-klustret. Använd följande kommando för att kontrollera ingångskontrollen:

```
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
```

Om alla poddar är i tillståndet `Running`, kontrollera loggarna för ingångskontrollen för att identifiera problemet med följande kommando:

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

Kommandot ovan följer ingångskontrollens loggar före poddarna och visar loggarna i realtid. Försök att ansluta med URL och kontrollera loggarna för eventuella fel.

Man kan använda `grep` under kontrollen av loggarna för att undersöka det specifika värdnamnet som inte är tillgängligt för att identifiera problemet. Om loggarna för värdnamnet finns i loggarna ligger problemet troligtvis hos de komponenter i det centrala övervakningssystemet som tar emot trafiken.

3. Kontrollera att central-hubbens ingång ska skapas med port 443, såsom visas nedan.

```
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. Om den skapas, kontrollera om central-hub-tls hemlighet ska skapas

```
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. Kontrollera loggarna för de felaktiga komponenterna i det centrala övervakningssystemet för att identifiera problemet med följande kommando:

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

ANNE View kan inte ansluta till det centrala övervakningssystemet

5.5 ANNE View kan inte ansluta till det centrala övervakningssystemet

1. Se till att ANNE View har giltiga SDC-certifikat.
2. Se till att ANNE View och det centrala övervakningssystemet finns i samma nätverk.
3. Kontrollera loggarna för poddarna till fleet-manager i klustret för att identifiera en möjlig orsak till problemet.

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

Kommandot ovan följer loggarna för SDC-podarna och visar loggarna i realtid. Försök att ansluta ANNE View till det centrala övervakningssystemet och kontrollera loggarna för eventuella fel.

5.6 Anslutningsproblem mellan poddarna i klustret medan poddarna körs på olika noder

1. Kubernetes-kluster använder overlay-nätverket för att ansluta poddar som körs på olika noder. Overlay-nätverket skapas av den CNI-plugin som är installerad på klustret. CNI-plugin ansvarar för att skapa nätverket och hantera nätverkstrafiken mellan poddarna.
2. Om poddarna inte kan kommunicera med varandra, kontrollera först nodernas status med följande 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. Om noderna är `Ready`, kontrollera statusen för CNI-poddarna med följande 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>
```

Om poddarna inte är i tillståndet `Running`, kontrollera loggarna för podden för att identifiera problemet med följande kommando:

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

5.7 Klustrets IP-adresser ändras efter att servern rebootats

VARNING: Försiktighetsåtgärder ska vidtas för att undvika att IP-adresserna för noderna i Kubernetes-klustret ändras efter att servern har rebootats. Se till att IP-adresserna som tilldelats Kubernetes-klusternoderna är statiska och inte tilldelas av DHCP-servern i nätverket.

Om IP-adresserna för noderna i Kubernetes-klustret ändras efter att servern har rebottats, ska Kubernetes-klustret återställas med de nya IP-adresserna. Följande steg ska vidtas för att återställa Kubernetes-klustret med de nya IP-adresserna:

1. Anslut till kontrollplansnoden i Kubernetes-klustret med SSH.
2. Skapa 'k3s_backup'-katalog

```
mkdir ~/k3s_backup
```

3. Kopiera k3s binärfil och installera skriptet till k3s_backup

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

4. Stoppa k3s tjänst

```
Kubectl stop k3s
```

5. Kör skriptet nedan för att först ta bort k3s

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

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

6. Installera nu k3s med ny IP

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

INSTALL_K3S_EXEC="server –disable traefik --node-ip {{ NEW_IP }} --advertise-address {{ NEW_IP }}" \

./tmp/install-k3s.sh

7. Kontrollera statusen för klusternoderna

```
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
```

Avsnitt 6. Sårbarhetsinformation

6.1 Sibel Healths policy för sårbarhetsinformation

Som leverantör av säker programvara, tjänster och forskning tar kundsupporten säkerhetsfrågor på allvar och inser vikten av integritet, säkerhet och kontakt med gemenskapen. Därför är kundsupporten engagerad i att åtgärda och rapportera säkerhetsproblem. Denna policy beskriver hur man rapporterar sårbarheter, vad man kan förvänta sig som gensvar och hur kundsupporten kommer att hantera dem.

6.2 Rapportering av säkerhetsproblem

Om man tror att man har upptäckt en sårbarhet i en produkt från kundsupporten, eller om man har ett säkerhetsproblem som man vill rapportera rapporterar man det enligt dessa steg:

- **E-post**: Skicka en detaljerad rapport till security@sibelhealth.com. Vid behov, använd vår offentliga PGP-nyckel nedan för att kryptera kommunikationen till oss.
    - Offentlig PGP-nyckel

```
-----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-----
```

- **Information att inkludera:**
    - En detaljerad beskrivning av sårbarheten, inklusive
        - Produktens eller tjänstens namn, URL och berörda versioner.
        - Operativsystem för involverade komponenter.
        - Datorn eller enhetens programkonfiguration vid tidpunkten för upptäckten.
        - Klass eller typ av sårbarhet (t.ex. med hjälp av en taxonomi som CWE).
        - Tid och datum för upptäckten.
    - Steg för att återskapa problemet
        - Teknisk beskrivning av utförda åtgärder, följd och resultat.
        - PoC kod/verktyg som användes för att producera det sårbara beteendet.
    - Uppskattning av potentiell påverkan och allvarlighetsgrad, om tillgänglig.
    - Potentiell grundorsak, om tillgänglig.

- Bedömning av omfattning, andra produkter, komponenter, tjänster eller leverantörer som tros vara berörda, om tillgängligt.
- Planer för offentliggörande, särskilt tidslinjer för embargo och publicering, om tillgängliga.

6.3 Vårt åtagande

När en sårbarhet rapporteras till kundsupporten åtar vi oss att:

- Bekräfta att rapporten mottagits inom 7 arbetsdagar.
- Bedöma och verifiera sårbarhetens legitimitet.
- Kategorisera sårbarhetens allvarlighetsgrad baserat på potentiell påverkan.
- Utveckla en åtgärdsplan baserad på allvarlighetsgraden och implementera en åtgärd.
- Ange en uppskattad tidslinje för åtgärden.
- Kommunicera framsteg via e-post under hela åtgärdsprocessen
- Rådgivande kommunikation med åtgärder enligt vår interna procedur för sårbarhetshantering.
- Behandla varje rapport konfidentiellt och inte lämna ut den till tredje part utan samtycke.
- Redovisa sårbarheter i informationen för släppta uppdateringar.

Observera att inte alla problem kommer att omfattas av Sibels process för sårbarhetsrapportering, däribland:

- Rapporter om saknade säkerhetsrubriker som inte leder till betydande påverkan eller prestandaförsämring.
- Föråldrade plattformsspecifika problem.
- Attacker genom social ingenjörskonst eller fysiska sårbarheter (t.ex. kontorssäkerhet).
- Problem med tredje parts tjänster som inte hanteras av kundsupporten

Avsnitt 7. Bilaga

7.1 Maskinläsbar 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