SIbEL

CENTRAL hub

GEBRAUCHSANWEISUNG

ANNE One Admin

support.sibelhealth.com

IFU P/N 443-00006-DE-A

Inhaltsverzeichnis

Abschnitt 1. Wichtige Sicherheitsinformationen

1.1 Übersicht

Dieses Dokument richtet sich an qualifiziertes technisches Personal, das für die Installation, Konfiguration, Wartung und Instandhaltung des ANNE One-Systems über den Administrator-Hub und dessen vernetzte Komponenten verantwortlich ist. Es beschreibt weder die klinische Anwendung noch die Patientenversorgung.

Zulässige Tätigkeiten umfassen:

- Installation und Konfiguration der Systemsoftware und der unterstützenden Infrastruktur gemäß den Anweisungen in dieser Gebrauchsanweisung und den zugehörigen Installationshandbüchern, insbesondere dem Installationshandbuch für das Central-Überwachungssystem SDD-SW-031-007.
- Systemüberwachung, Protokollprüfung, Sicherung, Wiederherstellung, Patch-Installation und Außerbetriebnahme, wie in diesem Dokument ausdrücklich beschrieben.
- Konfiguration der Zugriffskontrolle auf das Netzwerk, den Server und die Anwendungen gemäß den Empfehlungen.

Unzulässig sind unter anderem folgende Aktionen:

- Änderungen an der Software, Firmware, Systemarchitektur, den Sicherheitskontrollen oder Konfigurationen außerhalb der dokumentierten Verfahren.
- Verwendung von nicht dokumentierten Schnittstellen, Anmeldedaten oder Mechanismen für den Backdoor-Zugriff.
- Wartungsarbeiten, die zu einer Beeinträchtigung der klinischen Funktionalität, der Datenintegrität oder der Einhaltung gesetzlicher Vorschriften führen könnten.

Eine Hersteller-Autorisierung ist erforderlich:

- Für alle Abweichungen von dokumentierten Verfahren für Installation, Upgrades, Patching, Wiederherstellung oder Cybersicherheit.
- Für manuelle Eingriffe auf Datenbank-, Container- oder Betriebssystemebene, die nicht ausdrücklich in dieser Gebrauchsanweisung oder in der vom Hersteller bereitgestellten Servicedokumentation beschrieben sind.

1.2 Glossar

Tabelle 1: Glossar

Abkürzung	Definition
IFU	Gebrauchsanweisung (Instructions for use)
RBAC	Rollenbasierte Zugriffskontrolle (Role-Based Access Control)
ADT	Aufnahme-Entlassung-Verlegung (Admission-discharge-transfer)

PM	ANNE View
BLE	Bluetooth Low Energy
EOL	Ende der Lebensdauer (End of Life)
NFC	Nahfeldkommunikation (Near Field Communication)
LED	Leuchtdiode
IP	Ingress Protection (Schutzart)
IT	Informationstechnologie
VM	Virtuelle Maschine
TPM	Vertrauenswürdige Plattformmodule (Trusted Platform Modules)

1.3 Symbole

Tabelle 2: Symbole

Symbol	Titel	Beschreibung
Rx ONLY	Nur zur Anwendung nach ärztlicher Verschreibung	Dieses Gerät darf gemäß Bundesgesetz nur von einem zugelassenen Arzt oder auf dessen Anordnung hin verkauft werden.
	Gebrauchsanweisung beachten	Hinweis darauf, dass die Gebrauchsanweisung gelesen werden muss
	eIFU	Weist darauf hin, dass der Benutzer die Gebrauchsanweisung oder die elektronische Gebrauchsanweisung konsultieren muss.
QTY	Mengensymbol	Gibt die Anzahl der Einheiten oder Teile in der Verpackung an.
EC REP	Bevollmächtigter Vertreter in der Europäischen Union	Kennzeichnet den Bevollmächtigten in der Europäischen Union.
CE 2460	CE-Kennzeichnung	Zeigt an, dass ein Produkt vom Hersteller geprüft wurde und die Anforderungen der EU in Bezug auf Sicherheit, Gesundheit und Umweltschutz erfüllt. Diese Kennzeichnung ist für Produkte erforderlich, die weltweit hergestellt und anschließend in der EU vermarktet werden.

1.4 Herstellerinformationen

- Wenden Sie sich bei den folgenden Anliegen bitte an Ihren Kundendienst-Beauftragten:
    - Unterstützung bei der Einrichtung, Nutzung oder Wartung des Central-Überwachungssystems
    - Meldung unerwarteter Betriebszustände oder Ereignisse

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, 30175 Hannover
Deutschland

Abschnitt 2. Produktspezifikationen

2.1 Produktspezifikationen

Tabelle 3: Spezifikationen des Central-Überwachungssystems

	Central-Überwachungssystem (Server)
CPU	1 × 4 Core-CPU @ 2,4 GHz
RAM	6 GB
Festplattenkapazität	Betriebssystemfestplatte – 100 GB Datenfestplatte – 300 GB SSD
Externer Speicher	Keiner
Netzwerk	100/1000 MBit/s Ethernet
Weitere Hardware	Unterbrechungsfreie Stromversorgung
Betriebssystem	Ubuntu 24.04 Noble Numbat
Unterstützende Software	Keine

Tabelle 4: Spezifikationen des USB-Laufwerks für das Central-Überwachungssystem

Hersteller	iStorage
Modellnummer	IS-FL-DA3C-256-32
Speicherkapazität	32 GB
Schnittstelle	USB Typ C mit Typ-A-Adapter
Datenübertragungsrate	Lesen: 310 MB/s Schreiben: 246 MB/s
Abmessungen (mm)	Höhe: 80,10 mm Breite: 20,25 mm Tiefe: 10,70 mm
Gewicht	25 g
Betriebssystem – Kompatibilität	MS Windows, macOS, Linux, Chrome, Android, Thin Clients, Zero Clients, Eingebettete Systeme, Citrix und VMware
Verschlüsselungsschlüssel	256-Bit-Hardwareverschlüsselung

2.2 Sicherheitsempfehlungen

- Achten Sie darauf, die Festplattenverschlüsselung für die Betriebssystemfestplatte zu aktivieren, um die Datensicherheit zu gewährleisten.
- Aktivieren Sie vor der Installation TPM oder Secure Boot.
- Vor der Installation sollten auf den Hosts Antiviren- oder Anti-Malware-Tools implementiert werden.
- Drittanbieteranwendungen können nur dann mit dem Central-Überwachungssystem kommunizieren, wenn die Quell-IP-Adresse der Drittanbieteranwendung auf der Whitelist steht.
- Das Central-Überwachungssystem verwendet keinen Master-Schlüsselspeicher, um das Risiko von Brute-Force-Angriffen, unsicherer Speicherung und Seitenkanalangriffen zu vermeiden.
- Es wird empfohlen, regelmäßige Überwachungsdurchläufe und Datensicherungen durchzuführen.
- Richten Sie Beschränkungen für die Nutzung physischer oder tragbarer Geräte auf dem Server des Central-Überwachungssystems sowie auf dem Windows-System ein, das für die Überwachung verwendet werden soll.

2.3 Netzwerkempfehlungen

- Bitte stellen Sie sicher, dass sowohl das PMS als auch das Central-Überwachungssystem mit demselben lokalen Netzwerk (LAN) oder VLAN verbunden sind.
- Konfigurieren Sie Firewalls so, dass die Netzwerkgeschwindigkeit für erkannte Benutzer mit böswilligen Absichten eingeschränkt wird. Drosselung des Datenverkehrs der Benutzer auf 10 Megabit/Sekunde und Benachrichtigung der IT-Administratoren über böswillige Akteure.

2.3.1 Netzwerkportkonfiguration

Die Ports des Central-Überwachungssystems sind folgendermaßen konfiguriert. Bitte beachten Sie, dass alle nicht verwendeten Ports deaktiviert werden sollten.

Tabelle 5: Liste der Netzwerkportkonfigurationen und Beschreibung

Port	Quelle	Ziel	Beschreibung
53	Alle Kubernetes-Knoten	kube-dns/CoreDNS	DNS-Auflösung
80	Verschiedene Dienste	auth, central-monitoring, fleet-manager, kube-prometheus-stack-grafana	HTTP-Dienste
443	Verschiedene Dienste	kubernetes-dashboard, kubernetes API, metrics-server, kube-prometheus-stack-operator	HTTPS/API Zugang
8080	Interne Dienste	hmdm-headwind-mdm, kube-prometheus-stack-alertmanager, kube-prometheus-stack-kube-state-metrics, kube-prometheus-stack-prometheus	Interne Service-Endpunkte
31000	MQTT-Client	hmdm-headwind-mdm	MQTT-Kommunikation

Port	Quelle	Ziel	Beschreibung
5432	App-Dienste	PostgreSQL	Datenbankzugriff
6379	App-Dienste	Redis	Redis-Kommunikation
8443	Metriken-Scraper	kubegres-controller-manager-metrics-service	Metrik-Endpunkt
9090	Überwachungs-tools	kube-prometheus-stack-prometheus, prometheus-operated	Prometheus UI/API
9093	Alarmmanager	alertmanager-operated, kube-prometheus-stack-alertmanager	Alarmmanager-API
9094	Alarmmanager	alertmanager-operated, kube-prometheus-stack-grafana-headless	Cluster-Messaging (TCP)
9094	Alarmmanager	alertmanager-operated	Cluster-Messaging (UDP)
9100	Überwachungs-agenten	kube-prometheus-stack-prometheus-node-exporter	Knotenmetriken
9153	DNS-Metriken	kube-dns, kube-prometheus-stack-coredns	CoreDNS-Metriken
10250	Kubernetes-Komponenten	kube-prometheus-stack-kubelet	Sicherer Kubelet-Port
10255	Kubernetes-Komponenten	kube-prometheus-stack-kubelet	Kubelet-Port, schreibgeschützt
4194	Metrik-Agent	kube-prometheus-stack-kubelet	cAdvisor-Metriken
7946	Loki-Dienste	loki-memberlist	Kommunikation zur Clustermitgliedschaft
3100	Protokollierungs-dienste	loki, loki-headless	Loki-Protokolle
30080	Traefik	Traefik NodePort (HTTP)	HTTP-NodePort für eingehenden Datenverkehr
30443	Traefik	Traefik NodePort (HTTPS)	HTTPS-NodePort für eingehenden Datenverkehr

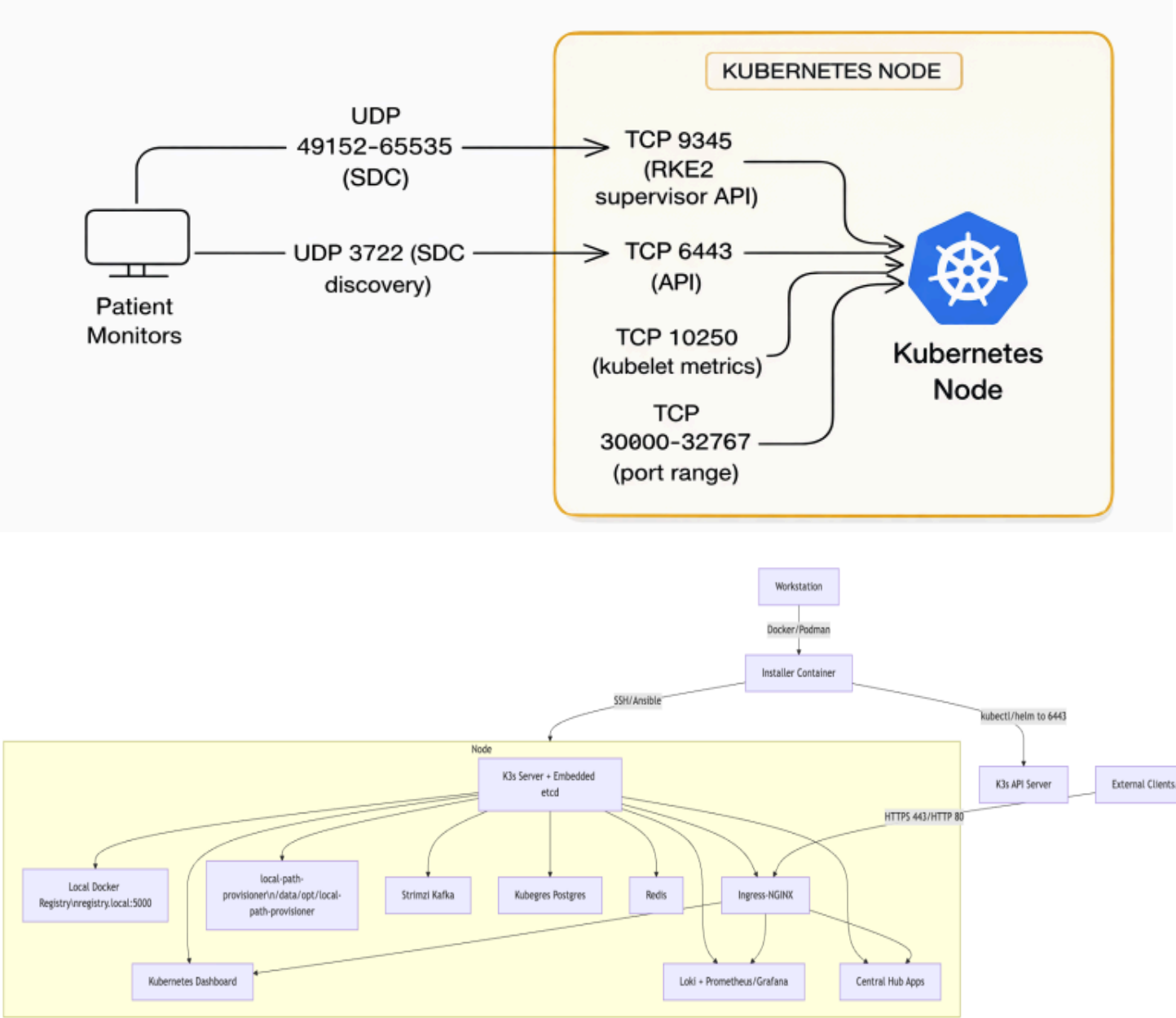


Abbildung 1: Netzwerkdiagramm des Clusters des Central-Überwachungssystems

Abschnitt 3. Administrator-Dashboards und -Dienst

3.1 Kubernetes-Dashboard

3.1.1 Zugriff auf das Kubernetes-Dashboard

Das Kubernetes-Dashboard ist über den folgenden Link erreichbar: https://dash.${your-domain-name}.

Um auf das Dashboard zugreifen zu können, müssen Sie sicherstellen, dass der DNS-Eintrag für diese Domain bei Ihrem DNS-Anbieter existiert.

Die Authentifizierung für das Dashboard kann mithilfe der während der Installation generierten ‚kubeconfig'-Datei oder mithilfe eines Tokens erfolgen.

Informationen zum Abrufen der ‚kubeconfig'-Datei finden Sie unter „Allgemeine Informationen zur Bereitstellung des Central-Überwachungssystems".

Der Token kann mit dem Tool kubectl wie folgt aus dem K8S-Cluster abgerufen werden:

Führen Sie bitte die folgenden Schritte aus, um auf das Dashboard-Token zuzugreifen:

1. Navigieren Sie nach Abschluss des Installationsvorgangs zu der Datei mit dem Namen `dashboard-token.txt`.
2. Diese Datei befindet sich im Ordner `„creds"` innerhalb des Installationsabbilds.
3. In dem Ordner `„creds"` werden alle Anmeldedateien gespeichert, einschließlich der Datei `dashboard-token.txt`.

3.1.2 Verwendung des Kubernetes-Dashboards

Das Central-Überwachungssystem umfasst ein Kubernetes(K8s)-Dashboard, um die Transparenz und Verwaltung des containerisierten Central-Überwachungssystems zu verbessern. Dieses Tool ist für die Aufrechterhaltung der Betriebsbereitschaft und der Compliance klinischer Systeme von entscheidender Bedeutung und liefert wichtige Einblicke und Kontrollmöglichkeiten für die Betriebsinfrastruktur.

Hauptmerkmale und Anpassungsmöglichkeiten::

- **Echtzeit-Cluster-Management**: Das K8s-Dashboard bietet einen Echtzeit-Überblick über den Zustand des Clusters, einschließlich Knotenstatus, Ressourcenauslastung und Leistung der bereitgestellten Anwendungen. Es ermöglicht Administratoren die effektive Überwachung und Verwaltung der Kubernetes-Cluster, die das Central-Überwachungssystem hosten.
- **Workload-Management**: Administratoren können Workloads, einschließlich Bereitstellungen, ReplicaSets und Pods, anzeigen, verwalten und Fehler beheben. Diese Funktionalität ist von entscheidender Bedeutung für den reibungslosen Ablauf klinischer Anwendungen und die Erfüllung der Leistungsanforderungen, die für eine sichere und effektive Versorgung der Patient*innen erforderlich sind.
- **Überwachung von Namespaces**: Das Dashboard ermöglicht die Überwachung verschiedener Namespaces und bietet eine segmentierte Ansicht des Clusters, die auf bestimmte klinische Anwendungen oder Abteilungen innerhalb der Gesundheitseinrichtung zugeschnitten werden kann.

- **Überwachung der Ressourcennutzung**: Es stehen detaillierte Kennzahlen zur CPU, Speicher und Speichernutzung zur Verfügung, die eine proaktive Verwaltung der Ressourcen ermöglichen. So lassen sich Leistungseinbußen vermeiden, die sich auf den klinischen Betrieb auswirken könnten.

3.1.3 Kompetenzen für IT-Administratoren in Krankenhäusern

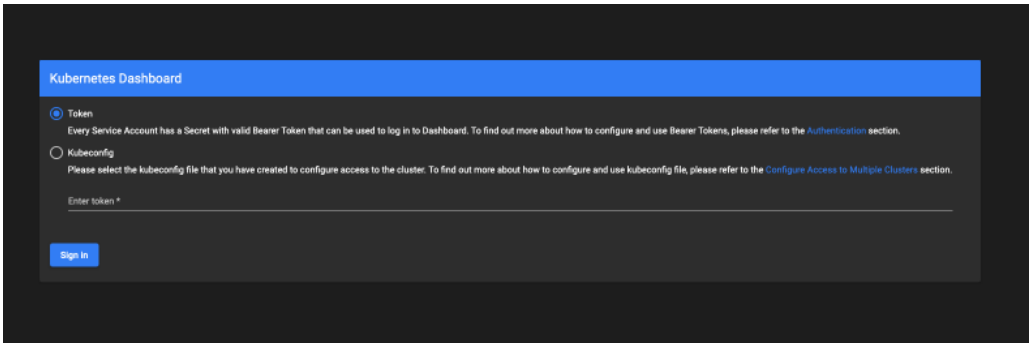
IT-Administratoren von Krankenhäusern sind befugt:

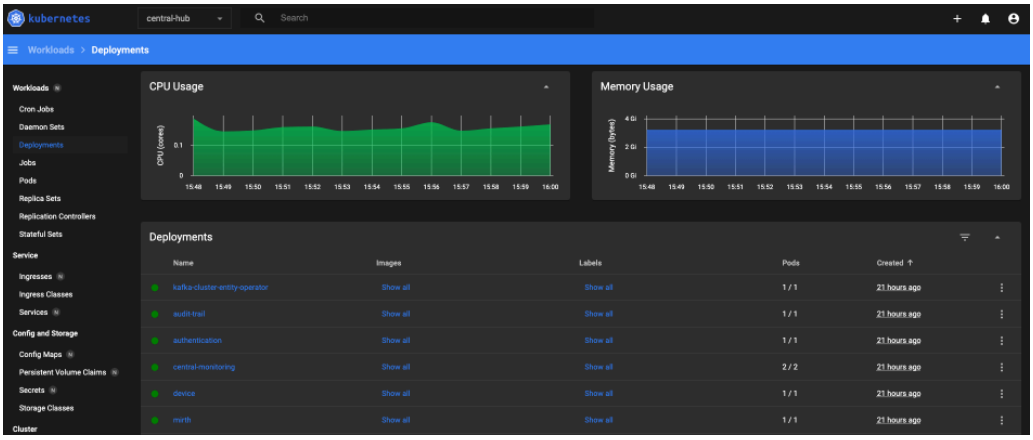
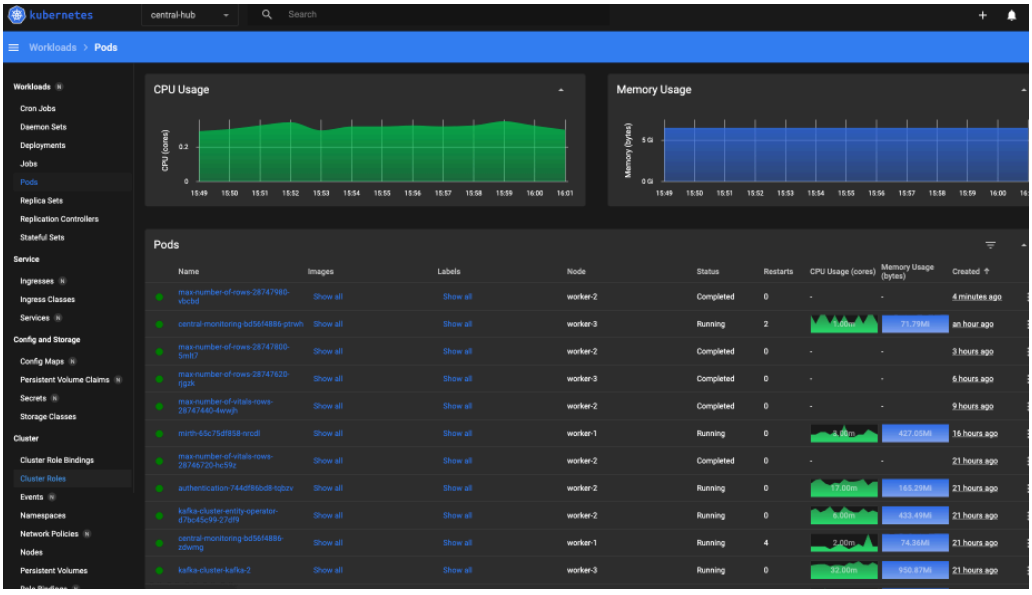
- **Anwendungen bereitzustellen und zu verwalten**: Das Dashboard vereinfacht die Bereitstellung und Verwaltung von Anwendungen innerhalb der Kubernetes-Umgebung. Administratoren können bestehende Dienste aktualisieren und Konfigurationen direkt über das Dashboard verwalten.
- **Clusterereignisse überwachen**: Das Dashboard bietet ein umfassendes Protokoll der Dienste des Central-Überwachungssystems, sodass Administratoren Änderungen verfolgen, die Protokolle exportieren und Probleme schnell diagnostizieren können. Dies trägt entscheidend dazu bei, die Compliance einzuhalten und zu gewährleisten, dass alle Probleme, die Anwendungen des Central-Überwachungssystems betreffen, umgehend behoben werden.
- **Verwaltung von Ressourcenkontingenten**: Administratoren können Ressourcenkontingente (Skalierung) festlegen und durchsetzen, um sicherzustellen, dass keine einzelne Anwendung oder kein einzelner Benutzer übermäßige Ressourcen verbraucht, wodurch die Leistung anderer wichtiger klinischer Anwendungen beeinträchtigt werden könnte.

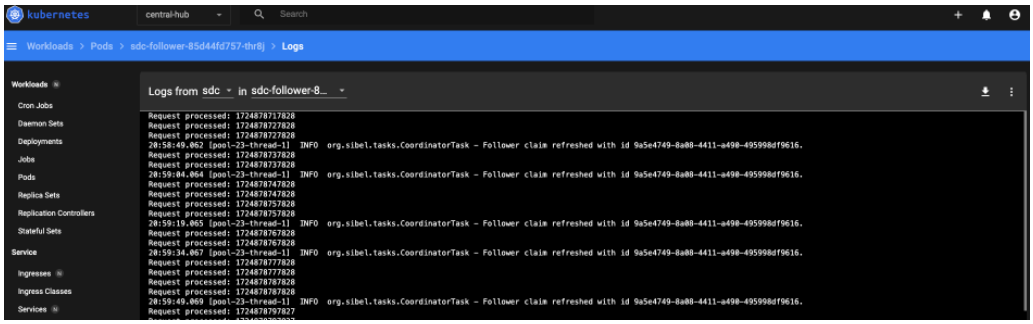
3.1.4 Überwachung von Metriken

- **Pod- und Containerüberwachung**: Kontinuierliche Überwachung des Pod-Status und des Containerzustands, um sicherzustellen, dass alle Komponenten klinischer Anwendungen ordnungsgemäß funktionieren.
- **Zustand und Leistung der Knoten**: Echtzeitüberwachung des Zustands der Knoten, einschließlich CPU und Speicher, um sicherzustellen, dass die Infrastruktur für klinische Anwendungen robust und zuverlässig bleibt.

Tabelle 6: Kubernetes-Überwachungsmetriken

K8s-Dashboard	Bild
Anmeldung	

Workload-Status	
Bereitstellungen	
Laufende Pods	

Serviceprotokolle	

3.2 Grafana-Dashboard

3.2.1 Zugriff auf das Grafana-Dashboard

Das Grafana-Dashboard kann über folgenden Link aufgerufen werden: https://mon.${your-domain-name}.

Um auf das Dashboard zugreifen zu können, müssen Sie sicherstellen, dass der DNS-Eintrag für diese Domain bei Ihrem DNS-Anbieter existiert. Wir empfehlen, eine Domain mit regulärem Ausdruck zu verwenden, damit Sie keine spezifische Domain bei Ihrem DNS-Anbieter hinzufügen müssen (z. B. *.{Ihr-Domain-Name}).

Führen Sie bitte die folgenden Schritte aus, um auf das Dashboard-Token zuzugreifen:

1. Navigieren Sie nach Abschluss des Installationsvorgangs zu der Datei mit dem Namen `monitoring.txt`.
2. Diese Datei befindet sich im Ordner „creds“ innerhalb des Installationsabbilds.
3. In dem Ordner `„creds“` werden alle Anmeldedateien gespeichert, einschließlich der Datei `monitoring.txt`.

3.2.2 Verwendung des Grafana-Dashboards

Das Central-Überwachungssystem für klinische Lösungen integriert erweiterte Funktionen zur Ereigniserkennung, Protokollierung, Alarmierung und Überwachung, die für die Gewährleistung der Zuverlässigkeit und Sicherheit klinischer Abläufe von entscheidender Bedeutung sind. Zu diesen Funktionen zählen Netzwerkabweichungen, Anmeldeversuche oder Änderungen der Systemkonfiguration. Diese Funktionen werden über den GPL-Stack – Grafana, Prometheus und Loki – bereitgestellt. Dieses Überwachungs-Toolset bietet eine umfassende Visualisierung in Form von Diagrammen, Grafiken und detaillierten Protokollanalysen und deckt alle Komponenten des Central-Überwachungssystems ab, einschließlich der Dienste des Central-Überwachungssystems, der Infrastrukturdienste, des Serververkehrs und der Netzwerküberwachung.

Hauptmerkmale und Anpassungsmöglichkeiten:

- **Vordefinierte Dashboards und Anpassungsoptionen**: Standardmäßig ist das System mit über 20 vordefinierten Dashboards ausgestattet, die vom Sibel-Team zusammengestellt wurden. Diese Dashboards bieten umfassende Einblicke in verschiedene Betriebsparameter. Darüber hinaus unterstützt die Überwachungsplattform die vollständige Anpassung von Dashboards und Alarmregeln, um spezifischen klinischen Anforderungen gerecht zu werden.
- **Protokollspeicherung**: Zur Optimierung von Speicherplatz und Leistung ist die standardmäßige Protokollspeicherdauer auf 7 Tage festgelegt. Dieser Zeitraum wurde unter Berücksichtigung eines

ausgewogenen Verhältnisses zwischen Speicherkapazität und dem Bedarf an historischen Daten in klinischen Umgebungen festgelegt.

- **Anmeldung**

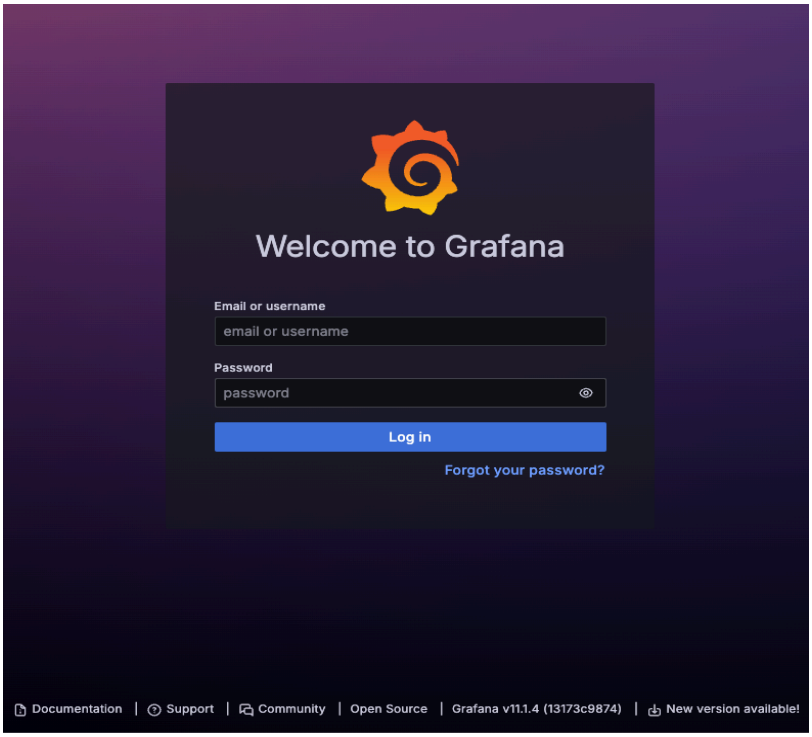


Abbildung 2: Die Versionsnummer von Grafana kann im Anmeldefenster überprüft werden.

3.2.2.1 Kompetenzen für IT-Administratoren

Befugnisse von IT-Administratoren:

- **Erstellung benutzerdefinierter Dashboards und Benachrichtigungen:** Administratoren können Dashboards entsprechend ihren betrieblichen Anforderungen gestalten und benutzerdefinierte Warnmeldungen einrichten, um eine proaktive Überwachung zu gewährleisten.
- **Benutzerverwaltung**: Das System unterstützt die rollenbasierte Zugriffskontrolle (RBAC), die es Administratoren ermöglicht, Benutzer mit entsprechenden Zugriffsebenen zu erstellen und zu verwalten, um einen sicheren und regelkonformen Betrieb zu gewährleisten.

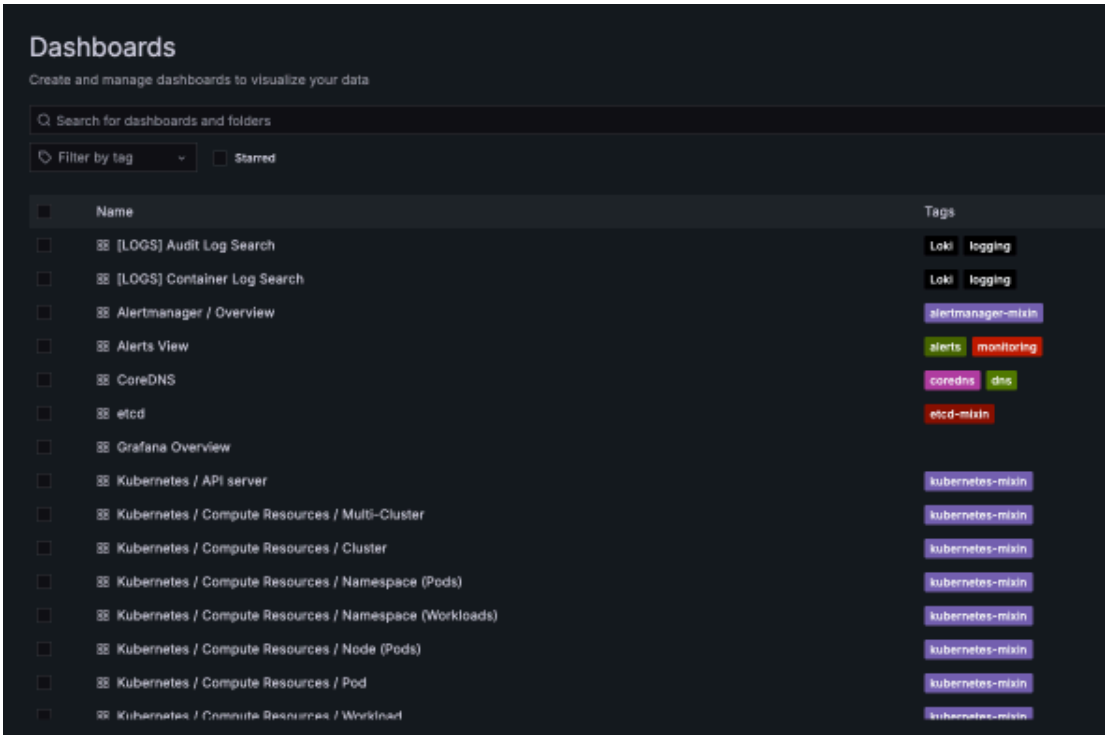
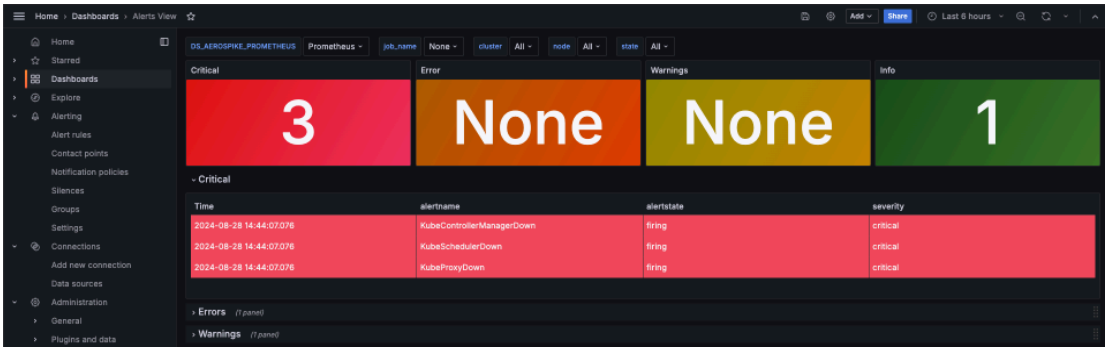
3.2.2.2 Überwachung von Metriken

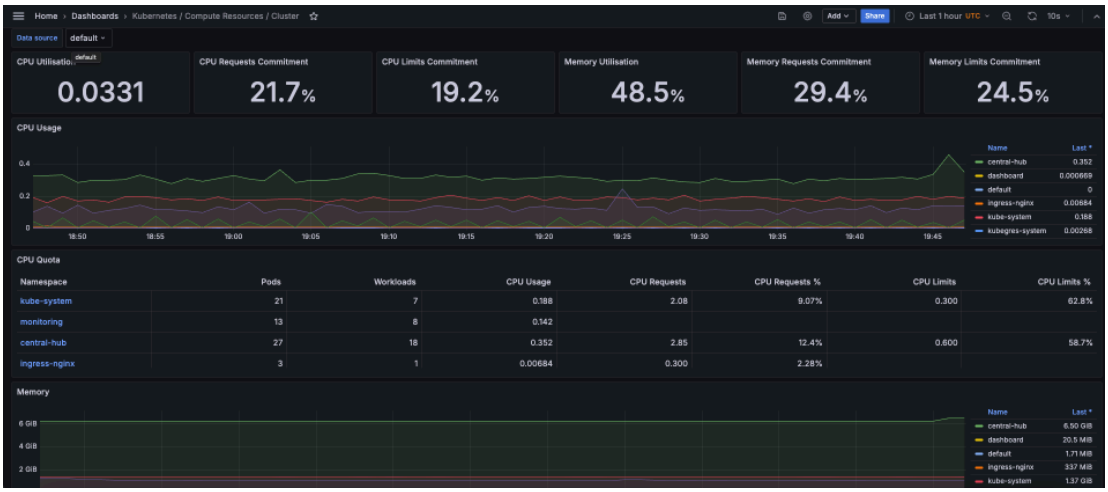
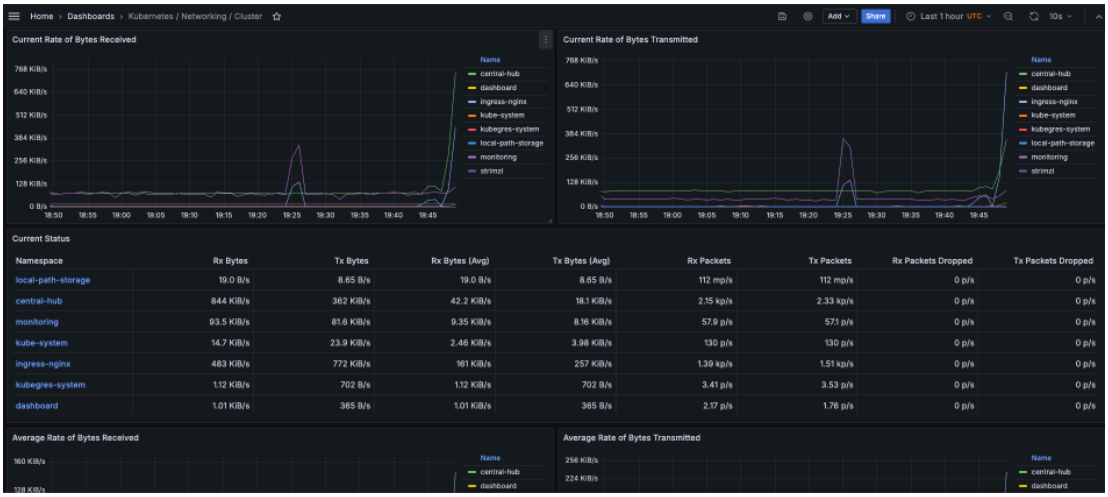
Das Überwachungstool bietet detaillierte Metriken und Protokolle, darunter:

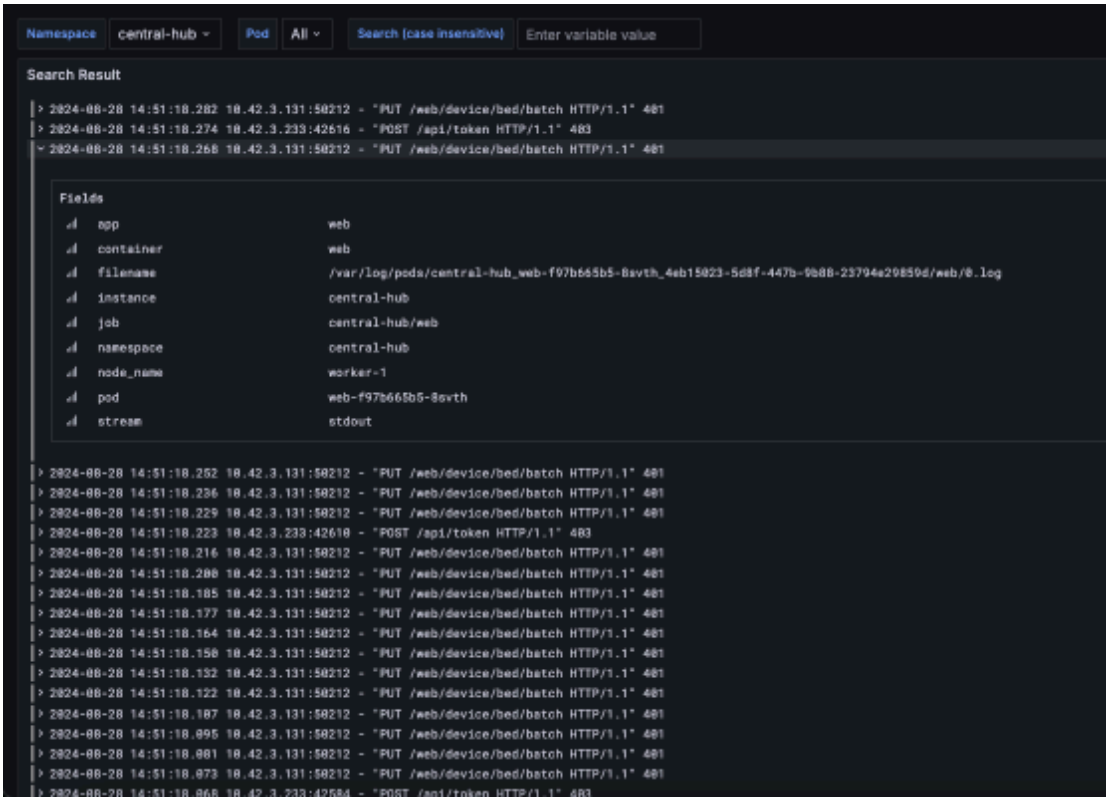
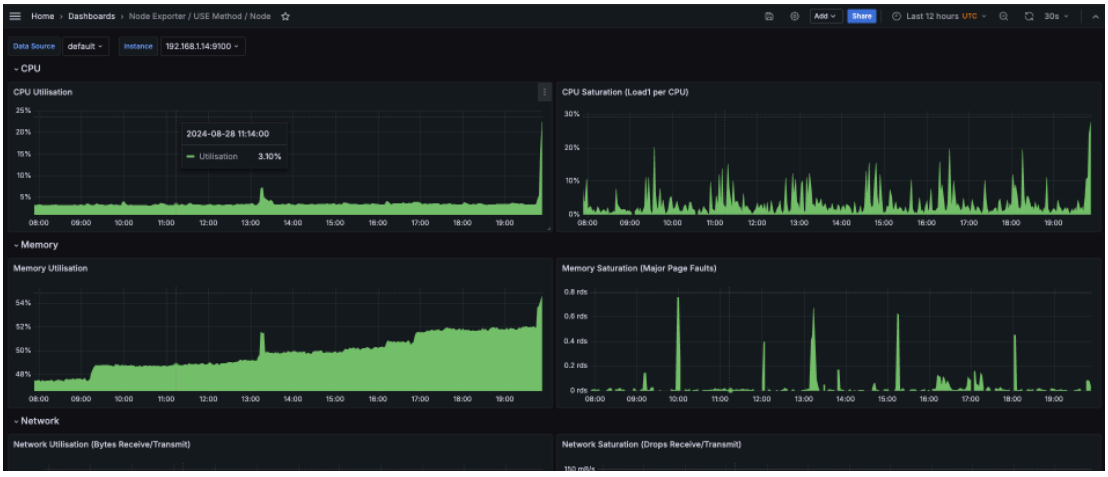
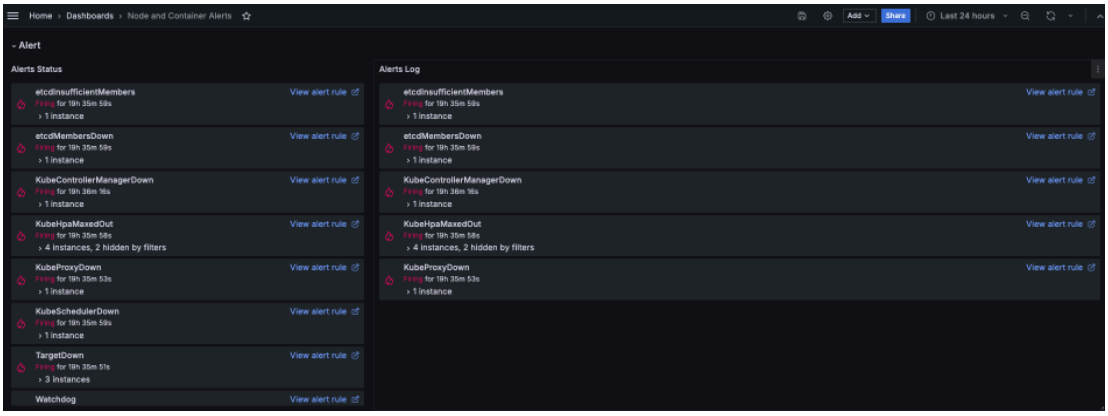
- **Statistiken zur Serververfügbarkeit**: Kontinuierliche Überwachung der Serververfügbarkeit und -betriebszeit zur Gewährleistung der Systemzuverlässigkeit.
- **Containerprotokollsuche**: Effiziente Suchfunktionen innerhalb von Containerprotokollen für eine schnelle Fehlerbehebung und Analyse.
- **Überwachung der Ressourcennutzung**: Echtzeitüberwachung der CPU-, Speicher- und Festplattenauslastung im gesamten System.
- **Cluster- und Knotenüberwachung**: Umfassende Einblicke in Clusterressourcen, Knotenleistung und den allgemeinen Systemzustand.

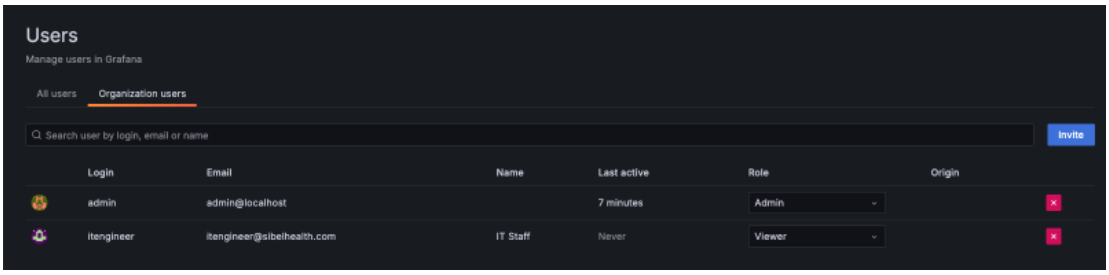
- **Überwachung der Netzwerkauslastung**: Detaillierte Überwachung des Netzwerkverkehrs, um Engpässe zu vermeiden und eine optimale Leistung sicherzustellen.
- **Prüf- und Proxy-Protokolle**: Führung detaillierter Prüfpfade und Proxy-Protokolle zur Unterstützung der Einhaltung klinischer und regulatorischer Standards.
- **Integration von Protokollabruf durch Anwendungen (Log Consumers)**: Das System lässt sich in kompatible Intrusion Detection(IDS)-Systeme (IDS) oder Security Information and Event Management(SIEM)-Lösungen integrieren.

Tabelle 7: Grafana-Überwachungsmetriken

Grafana	**Bild**
Dashboard	
Alarmansicht	

Clusterressource	
Vernetzung	

Containerprotokolle	
VM-Ressource	
Knoten- und Dienstwarnungen	

Benutzererstellung und -verwaltung (RBAC)	

Diese Überwachungslösung wurde entwickelt, um den sicheren, effizienten und konformen Betrieb von Central-Überwachungssystem-Systemen zu gewährleisten und entspricht den FDA-Richtlinien für medizinische Software.

3.2.3 Speichern von Protokollen

Das System speichert Protokolle in unverarbeitetem (rohem) und im JSON-Format:

- Unverarbeitete (Roh-)Protokolle sind wie folgt formatiert:
- Die Protokolle des Lastverteilers liegen im JSON-Format vor:

Die Administrator-Agenten innerhalb des Kubernetes-Clusters weisen die Container-Laufzeitumgebung an, die Protokolle auf Anwendungsebene in das Verzeichnis `/var/log/pods` zu schreiben. Zusätzlich werden die Systemprotokolle des Kubernetes-Clusters unter `/var/lib/rancher/rke2/server/logs` gespeichert.

Die Protokolle werden hier abhängig vom verfügbaren Speicherplatz rotiert. Standardmäßig ist folgende Rotationskonfiguration eingestellt:

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

Der Protokollsammlungsagent Promtail bezieht die Anwendungsprotokolle in `/var/log/pods` von jedem Kubernetes-Knoten und die Protokolle auf Systemebene in `/var/lib/rancher/rke2/server/logs` von den Kontrollebenen-Knoten und überträgt sie anschließend an Loki, das als Datenbank für Protokolle dient.

Die Protokolle auf Netzwerkebene der Lastverteiler-VM werden im Verzeichnis `/var/lib/docker/containers/` gespeichert. Der Promtail-Agent läuft parallel dazu und überträgt die Daten anschließend an Loki.

3.2.4 Problembehebung bei Geräteereignissen

Wenn ungewöhnliche Ereignisse festgestellt werden, reagiert das System entsprechend. Bei wiederholten Anmeldeversuchen, beispielsweise fünf aufeinanderfolgenden fehlgeschlagenen Anmeldeversuchen, sperrt das System weitere Anmeldeversuche für 15 Minuten.

Alle unbekannten Entitäten ohne gültige Zertifikate werden auf eine Sperrliste gesetzt und werden von der Kommunikation mit dem System ausgeschlossen. Erkennt das System zudem einen übermäßigen Netzwerkverkehr, der den normalen Betrieb beeinträchtigt, unterbricht es das Daten-Streaming und benachrichtigt die Endbenutzer per Fehlermeldung über das Netzwerkproblem. Dies hat keine Auswirkungen auf die Verbindung zwischen den Sensoren und ANNE View. Diese Anomalien werden in Echtzeit überwacht und mithilfe des Central-Überwachungssystems protokolliert.

3.3 Lokales MDM-Dashboard

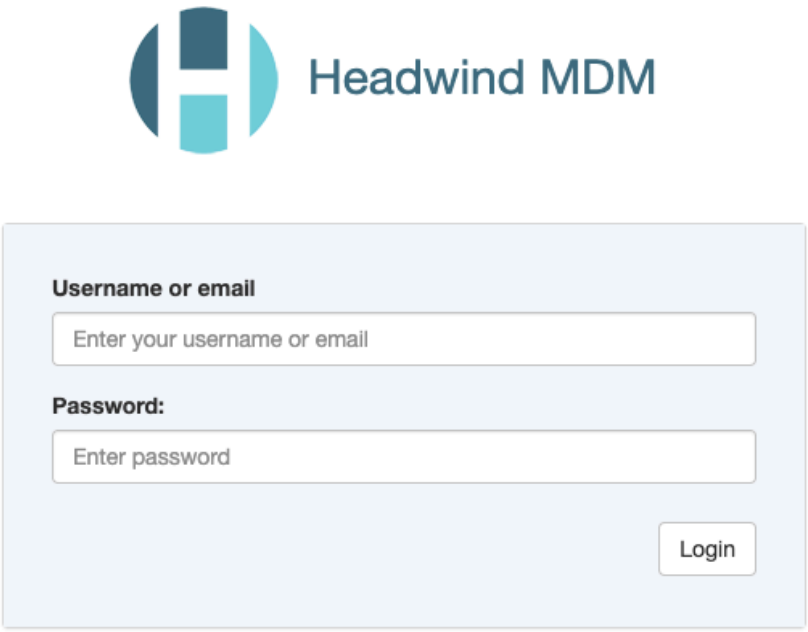
Das lokale MDM-Dashboard kann über folgenden Link aufgerufen werden: https://hmdm.${your-domain-name}.

Um auf die Dashboard-Oberfläche zugreifen zu können, muss die folgende Konfiguration vorhanden sein: Über Ihren DNS-Anbieter muss ein DNS-Eintrag für die angegebene Domain erstellt werden. Ohne diesen Eintrag wird die Dashboard-URL nicht korrekt aufgelöst.

Authentifizierung:

- Bitte verwenden Sie die E-Mail-Adresse des zugewiesenen technischen Benutzers als Benutzernamen.
- Das Standardpasswort lautet: admin.

Nach der ersten erfolgreichen Anmeldung fordert das System den Benutzer auf, **ein neues Passwort zu erstellen**. Dies ist ein obligatorischer Schritt, um weiterhin Zugriff zu erhalten.



Figur 3: Anmeldeschnittstelle für das lokale MDM-Dashboard

3.3.1 MDM-Lizenz und Geräteregistrierung

Der IT-Administrator muss über einen gültigen Lizenzschlüssel verfügen, um die volle Funktionalität des MDM-Systems nutzen zu können. Dieser Lizenzschlüssel muss nach Abschluss der CMS-Installation und Lieferung durch den Hersteller eingegeben werden.

Geräteregistrierung und -konfiguration:

Über die lokale MDM-Schnittstelle kann der IT-Administrator folgende Aufgaben ausführen:

- ANNE View-Geräte unter Verwendung der von Sibel Health bereitgestellten Konfigurationseinstellungen registrieren.
- Die Anne-View-Anwendung auf den registrierten Geräten installieren.
- Den Kioskmodus aktivieren und konfigurieren, um sicherzustellen, dass das Gerät auf die vorgesehene klinische Einsatzumgebung beschränkt ist.

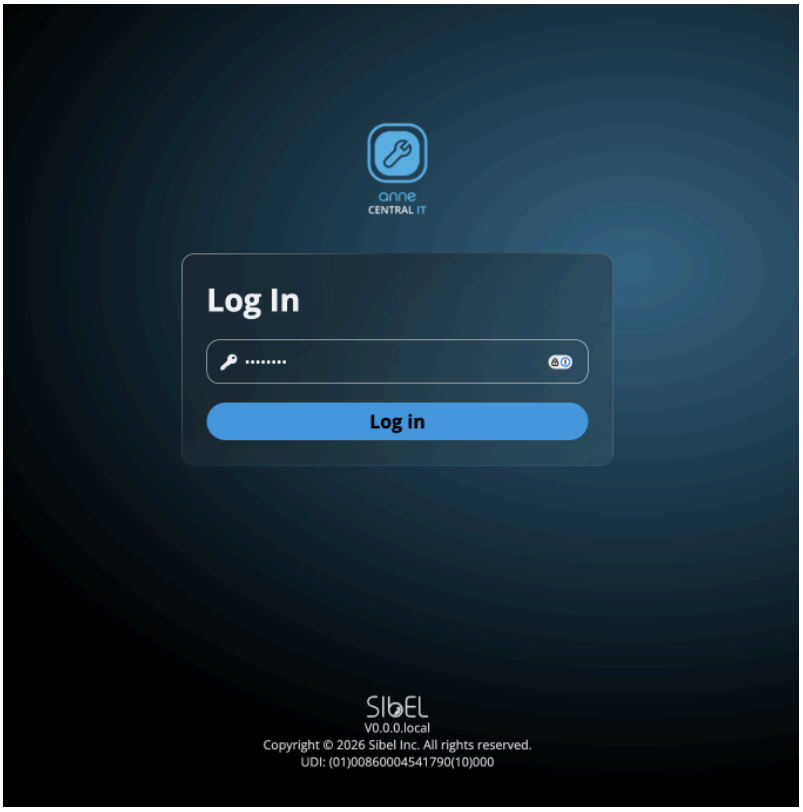
Um einen sicheren und stabilen Betrieb der Geräteverwaltung zu gewährleisten, sind eine ordnungsgemäße Lizenzierung und Konfiguration nach der Installation erforderlich.

3.4 Admin-Hub

3.4.1 Anmeldung

Der Admin-Hub kann über folgenden Link aufgerufen werden: https://cms.${your-domain-name}.

Geben Sie Ihr Passwort ein, um sich im Central Hub anzumelden. Klicken Sie auf die Schaltfläche „Anmelden“.



Hinweis: Der IT-Administrator konfiguriert das Benutzerkonto und das Passwort während der Installation.

3.4.2 Fehlerbehebung

Tabelle 8: Fehlerbehebung bei der Anmeldung im Admin Hub

Fehlermeldung	Grundursache	Empfohlene Benutzeraktion
Serverfehler. Bitte versuchen Sie es in wenigen Minuten erneut.	Serverfehler des Systems.	Versuchen Sie es später erneut oder überprüfen Sie den Servicestatus. Sollte das Problem weiterhin bestehen, wenden Sie sich bitte an den Support von Sibel Health.
Falsches Passwort. Bitte versuchen Sie es erneut.	Der Benutzer hat ein falsches Passwort eingegeben.	Versuchen Sie es erneut mit dem richtigen Passwort.
Zu viele Versuche. Bitte versuchen Sie es in 15 Minuten erneut.	Der Benutzer hat das Passwort mindestens 5 Mal falsch eingegeben.	Versuchen Sie es nach 15 Minuten erneut. Falls Sie Ihr Passwort vergessen haben, setzen Sie es zurück.

3.4.3 Dashboard für die Sensorlebensdauer

Nach erfolgreicher Anmeldung kann der IT-Administrator:

- Sich eine Liste der im CMS registrierten Geräte anzeigen lassen.
- Der Admin Hub zeigt Informationen wie Seriennummer, Gerätetyp, Alter des Geräts, Ablaufstatus und den zuletzt angezeigten Zeitstempel an.
- Die folgenden Filter sind für den Benutzer für eine vereinfachte Nutzung verfügbar: Betriebsstatus, Ablaufstatus innerhalb von 7 Tagen, kürzlich in den letzten 24 Stunden hinzugefügt, Seriennummer oder Gerätetyp.
- Das Alter des Geräts und der Ablaufstatus sind für Geräte, die nicht von Sibel hergestellt wurden, möglicherweise nicht verfügbar; dies betrifft Patientenüberwachungsgeräte und OEM-Geräte.

Hinweis: Patientenüberwachungsgeräte und Sensoren werden im Folgenden zusammenfassend als „das Gerät“ bezeichnet.

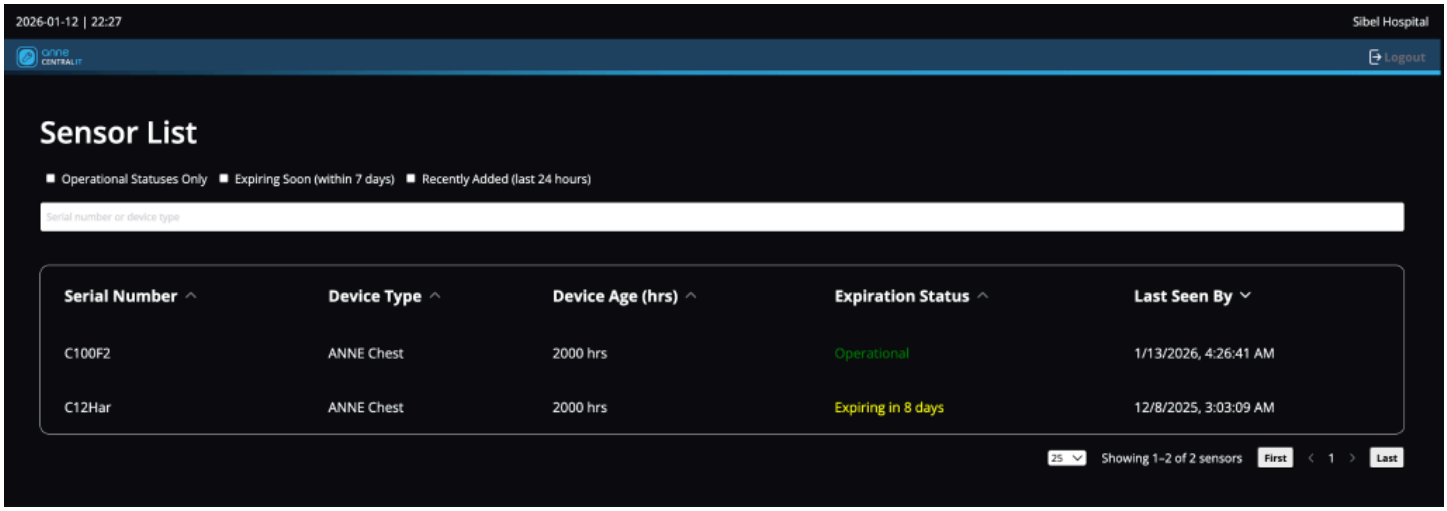
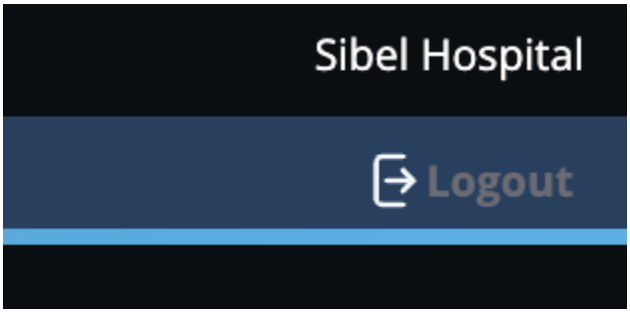


Abbildung 4: Dashboard für die Sensorlebensdauer

3.4.4 Abmelden

Klicken Sie auf die Schaltfläche „Abmelden“ in der oberen rechten Ecke.



Hinweis: Der IT-Administrator wird nach 15 Minuten ohne Aktivität automatisch abgemeldet.

Abschnitt 4. Wartung des Central-Überwachungssystems

4.1 Wartung des Central-Überwachungssystems

4.1.1 Cybersicherheitsaspekte des Central-Überwachungssystems

Um ein Höchstmaß an Sicherheit zu gewährleisten, empfiehlt Sibel Health die folgenden Sicherheitsvorkehrungen für die Installation des ANNE View- und Central-Überwachungssystems.

- Die Authentifizierung zwischen ANNE View und dem zentralen Server erfolgt über eine X.509 Certificate Chain auf Basis von Zertifikaten und Kettenvalidierung. Es werden ausschließlich eingehende Anfragen von ANNE View durch den Central-Server validiert. Es wird empfohlen, Zertifikate mit einer Gültigkeitsdauer von einem Jahr zu erstellen und dabei openssl mit RSA:4096-Verschlüsselung zu verwenden.
- Es werden keine PHI-Daten in der Datenbank des Central-Überwachungssystems gespeichert.
- Für die sichere Datenübertragung zwischen dem Webportal des Central-Überwachungssystems und dem Backend-Gateway wird ein JSON-Webtoken verwendet. Das Token ist 15 Minuten lang, das Refresh-Token 7 Tage lang gültig.
- Das Central-Überwachungssystem verwendet keinen Master-Key-Speicher, um das Risiko von Brute-Force-Angriffen, unsicherer Speicherung und Seitenkanalangriffen zu vermeiden.
- Sibel Health empfiehlt, die Gültigkeitsdauer von Zertifikaten auf mindestens 6 Monate und höchstens 1 Jahr festzulegen, um ein ausgewogenes Verhältnis zwischen Sicherheit und betrieblicher Effizienz zu gewährleisten.

4.1.2 Sicherheitspatches für das Central-Überwachungssystem

Explizite Patches, die entdeckte Schwachstellen beheben, sind unbedingt erforderlich und sollten unverzüglich nach Erhalt installiert werden. Diese sicherheitsrelevanten Patches enthalten keine neuen Funktionen und sollten als eigenständige Patches installiert werden, um das Produkt vor der jeweiligen Sicherheitslücke zu schützen.

Nach Fertigstellung und Genehmigung eines Patches erfolgt die Verteilung des Patches durch Sibel Health an die Kunden über einen sicheren, hardwareverschlüsselten USB-Stick.

Sicherheitspatches für das Central-Überwachungssystem können von einem IT-Administrator mit Zugriff auf die Installation des Central-Überwachungssystems installiert werden. Die Schritte zur Anwendung der Sicherheitspatches für das Central-Überwachungssystem entsprechen exakt den Schritten zur Aktualisierung des Central-Überwachungssystems, wie in Abschnitt 5 (Seite 35) des SDD-SW-031-007-Dokuments „Installationshandbuch für das Central-Überwachungssystem" beschrieben.

Die neueste Version kann über das K8s-Dashboard durch Überprüfung der Image-Version verifiziert werden.

4.1.3 Patches für das Central-Überwachungssystem

Die Häufigkeit der Patchinstallationen für Aktualisierungen des Central-Überwachungssystems folgt einem zweiwöchigen Sprint-Zyklus und einem Hotfix-Prozess. Die Verteilung der Patches erfolgt durch Sibel Health.

4.1.4 Versionsfreigabe des Central-Überwachungssystems

Die Vollversionen des Central-Überwachungssystems werden auf Grundlage des internen Entwicklungszyklus von Sibel Health erstellt. Der Versionsfreigabeprozess durchläuft die entsprechenden Testphasen (Verifizierung und

Validierung), damit eine Version mit neuen Funktionen, Korrekturen von Anomalien aus früheren Versionen sowie Leistungsverbesserungen erstellt werden kann. Die Verteilung der Versionen erfolgt durch Sibel Health.

4.1.5 Datensicherung und Wiederherstellung des Central-Überwachungssystems

Nach der Inbetriebnahme des Central-Überwachungssystems müssen Datenbanksicherungen aktiviert werden. Da diese Installation keine Integration mit einem externen Datenspeicher umfasst, wird die automatische Datensicherung nicht unterstützt. Im Rahmen der Notfallwiederherstellung ist es erforderlich, die Datenbank wöchentlich manuell zu sichern.

Die Datensicherungen sollten sowohl vor Ort als auch außerhalb des Standorts gespeichert werden, um Datenredundanz und -sicherheit zu gewährleisten. Datensicherungen sollten außerhalb der Spitzenzeiten geplant werden, um die Auswirkungen auf den laufenden Betrieb zu minimieren. Eine regelmäßige Überwachung ist unerlässlich, um die Integrität und Zuverlässigkeit der Datensicherungen zu validieren.

Für den Fall eines kritischen Funktionsausfalls finden Sie detaillierte Anweisungen zur Sicherung/Wiederherstellung in Abschnitt 3.1.3 (Seite 28) des SDD-SW-031-007 Installationshandbuchs für das Central-Überwachungssystem. Die oben genannten kritischen Funktionen können ebenso wenig wie die Beschreibung der zulässigen Kommunikationsports in Abschnitt 4.1 von nicht autorisierten Benutzern konfiguriert werden.

Das Central-Überwachungssystem besteht aus einer Reihe virtueller Maschinen, auf denen der Kubernetes-Cluster läuft. Die Clusterknoten speichern ein Abbild der Konfiguration jedes einzelnen Knotens im Cluster auf unbestimmte Zeit. Im Rahmen der automatischen Wiederherstellung werden die Dienste des Central-Überwachungssystems auf Pods auf Worker-Knoten ausgeführt. Sollte einer der Dienste (Pods) ausfallen, wird durch die Ausfallsicherung und Wiederherstellung über Cluster-Dienste ein Ersatz für den ausgefallenen Pod mit seiner ursprünglichen Konfiguration erstellt. Dadurch wird die volle Kapazität und Funktionalität des Clusters wiederhergestellt.

Sollte ein Fall auftreten, der eine manuelle Wiederherstellung einer Konfiguration erfordert, kann ein authentifizierter und autorisierter Administrator die Konfiguration von einem anderen Knoten kopieren, um die volle Kapazität und Funktionalität des Clusters wiederherzustellen.

4.1.6 Ereignisprotokollierung des Central-Überwachungssystems

Sibel Health bietet innerhalb seiner Systeme und Subsysteme Funktionen zur Protokollierung und Überwachung von Prüfpfaden. Diese Protokolle und Metriken liefern Informationen zum Zustand der Systeme, zu deren Leistungskennzahlen sowie zu Anomalien oder Problemen innerhalb der Systemkomponenten. Diese Ereignisse sind als administrative Funktion im Admin-Dashboard verfügbar, um Status, Protokolle, Metriken und Grafiken zu überprüfen.

IT-Administratoren in Krankenhäusern müssen die Protokolle regelmäßig im Rahmen eines Standardverfahrens zur kontinuierlichen Überwachung überprüfen.

4.1.7 Kryptografiekontrolle des Central-Überwachungssystems

Sibel Health verwaltet den Lebenszyklus von Schlüsseln und Zertifikaten über geeignete kryptografische Module wie 1Password. Diese Module bieten Verschlüsselung, Zugriffskontrolle und eine sichere Speicherung sensibler Daten. Alle kryptografischen Assets werden vom Informationssicherheitsmanager von Sibel in Übereinstimmung mit den Empfehlungen der Sicherheitsstandards NIST SP 800-131A, „Transitioning the Use of Cryptographic Algorithms and Key Lengths" (Umstellung der Verwendung von kryptografischen Algorithmen und Schlüssellängen) und FIPS 140-3, „Security requirements for Cryptographic Modules" (Sicherheitsanforderungen für kryptografische Module) verwaltet und gepflegt.

4.1.7.1 Speicherung kryptografischer Assets

Sibel Health speichert und verwaltet kryptografische Assets, Schlüssel und Zertifikate in den sicheren Tresoren von 1Password. Dabei kommen hochmoderne Verschlüsselungsalgorithmen zum Einsatz, um unbefugten Zugriff zu verhindern und den kontrollierten Zugriff ausschließlich auf autorisiertes Personal zu beschränken. 1Password gewährleistet die verschlüsselte Sicherung der gespeicherten Assets, um den Ausfallsicherungsmechanismus zu unterstützen.

Falls Kunden aufgrund interner Cybersicherheitsanforderungen ihrer Organisation die Kontrolle über Kryptografie-Assets verlangen, informiert Sibel Health die Kunden über die Anwendung geeigneter Kryptografiemodule gemäß den Best Practices für Cybersicherheit, wie beispielsweise dem aktuellen US-Standard zur Validierung kryptografischer Module in Hard- und Software „FIPS 140-3 Sicherheitsanforderungen für Kryptografiemodule“.

- FIPS 140-3 (FIPS 140-2 Abschnitt 4.7) beschreibt Anforderungen hinsichtlich der Verwaltung kryptografischer Schlüssel.

4.1.7.2 Zugriffskontrolle für kryptografische Assets

Alle kryptografischen Assets müssen verschlüsselt werden, und der Zugriff muss anhand einer rollenbasierten Zugriffskontrollrichtlinie (RBAC) durch den von Sibel benannten IT-/Sicherheitsmanager streng kontrolliert werden. Sibel Health befolgt die von FIPS 140-3 empfohlene Zugriffskontrollrichtlinie.

Sibel Health gibt Kunden auch Empfehlungen für die entsprechende Gestaltung ihrer Zugriffskontrollrichtlinien an die Hand. Die Empfehlung von Sibel Health berücksichtigt die folgenden Rollen und Dienste:

- IT-Administrator (Superuser)
    - Fungiert als Superuser, regelt die Zugriffskontrollrichtlinie und verwaltet den Lebenszyklus von kryptografischen Assets.
- Medizinisches Fachpersonal (Benutzer)
    - Fungiert als Benutzer und hat Zugriff auf die klinischen Passwörter des Central-Überwachungssystems.

4.1.7.3 Erstellung und Erneuerung (Rotation) von kryptografischen Assets

Kryptografische Schlüssel und Zertifikate werden vor und während der Bereitstellung des Central-Überwachungssystems generiert.

Folgende Schlüssel und Zertifikate werden vor der Bereitstellung benötigt:

- Digitale Signaturschlüsselpaare für die ANNE View- und Central-Überwachungssystem-Software
- TLS/SSL Certificate Chain für sichere Netzwerkkommunikation innerhalb des Central-Überwachungssystems
- Die RootCA- und IntermediateCA-Zertifikatskette von Sibel gewährleistet die sichere Authentifizierung und Kommunikation zwischen ANNE View und dem Central-Überwachungssystem.

Wenn ein Kunde eine eigene Kryptografieverwaltung wünscht, stellt Sibel Health dem IT-Administrator des Kunden die folgenden Informationen zur Verfügung:

- Kryptografiealgorithmus und Protokolle
- Gültigkeit der Kryptografie

Wenn die Gültigkeit der Kryptografie bald abläuft, erneuert oder rotiert Sibel Health die Schlüssel und Zertifikate gemäß NIST SP 800-57 Teil 1 (Empfehlung für die Schlüsselverwaltung) und NIST 1800-16B (Sicherung von Webtransaktionen).

Sibel Health wird die Gültigkeit von Schlüsseln und Zertifikaten über das kryptografische Modul 1Password nachverfolgen. Dieses Modul wird so konfiguriert, dass es den IT-/Sicherheitsmanager oder Cybersicherheitsingenieur von Sibel Health 30 Tage vor der Schlüsselrotation oder Zertifikatserneuerung benachrichtigt.

IT-Administratoren von Kunden wird empfohlen, die Schlüsselrotation des Central-Überwachungssystems gemäß der in Tabelle 9 beschriebenen Cryptoperiod durchzuführen.

Tabelle 9: Empfehlung zur Cryptoperiod und Gültigkeit von Zertifikaten nach Asset-Typ gemäß NIST SP 800-57 Teil 1 und NIST SP 1800-16B

Asset-Name	**Asset-Typ**	**Gültigkeit/Cryptoperiod**
Schlüssel		
Digitale Signatur	Privater Signaturschlüssel	1 bis 3 Jahre
Digitale Signatur	Öffentlicher Signaturverifizierungsschlüssel	Nicht spezifiziert, aber folgt dem privaten Schlüssel (1 bis 3 Jahre).
Benutzerauthentifizierung	Privater Authentifizierungsschlüssel	1 bis 2 Jahre
Benutzerauthentifizierung	Öffentlicher Authentifizierungsschlüssel	1 bis 2 Jahre
PostgreSQL-Verschlüsselungs-schlüssel	Symmetrische Datenverschlüsselungsschlüssel	3 Jahre
Passwort		
PostgreSQL-Authentifizierungs-schlüssel	Passwort	1 Jahr
Redis-Authentifizierungsschlüssel		
Administratorpasswort		
Admin-Dashboard-Token		
Passwort für das Überwachungs-Dashboard		
Zertifikat		
TLS/SSL Zertifikat	Zertifikat	1 Jahr
IntermediateCA-Zertifikat		

Um eine sichere Kommunikation und Kryptografie innerhalb des Systems zu gewährleisten, ist es erforderlich, Zertifikate rechtzeitig zu erneuern und Schlüssel zu rotieren. Zertifikate sollten mindestens 30 Tage vor Ablauf des aktuellen Zertifikats erneuert und validiert werden. Schlüssel sollten entsprechend der Cryptoperiod rotiert werden. Sibel Health orientiert sich bei der Erneuerung von Zertifikaten an der Richtlinie NIST SP 1800-16B.

Die folgenden Schritte beschreiben den Prozess zur Erneuerung von Zertifikaten und deren Zustellung an die Kunden:

- **Überwachung des Ablaufdatums von Zertifikaten**: Das IT-/Sicherheitsteam von Sibel Health überprüft monatlich das Ablaufdatum der Zertifikate über das Kryptografiemodul 1Password. Bei einer Selbstverwaltung der Zertifikate durch den Kunden verlangt Sibel Health von dessen IT-Administratoren, die Gültigkeitsdauer der Zertifikate regelmäßig zu überprüfen.

- **Generierung einer Zertifikat-Signierungsanforderung (CSR)**: Erstellen Sie eine neue CSR für die Zertifikatserneuerung. Verwenden Sie vorhandene private Schlüssel oder generieren Sie neue, um ein neues Zertifikat zu erhalten.
- **Übermittlung der CSR an die Zertifizierungsstelle (CA)**: Übermitteln Sie die CSR an eine vertrauenswürdige CA.
- **Erhalt eines neuen Zertifikats**: Sobald die Validierung abgeschlossen ist, erhalten Sie die neuen Zertifikate**.**
- **Auslieferung des neuen Zertifikats**: Das IT-/Sicherheitsteam von Sibel Health leitet die erneuerten Zertifikate über 1Password an die IT-Administratoren der Kunden weiter.
- **Ersatz von Zertifikaten**: Das IT-/Sicherheitsteam von Sibel Health kommuniziert mit den IT-Administratoren des Kunden unter strikter Einhaltung von Abschnitt 4.5 (Seite 34) des SDD-SW-031-007-Installationshandbuchs des Central-Überwachungssystems, um einen erfolgreichen Ersatz der Zertifikate zu gewährleisten.
- **Installation des Zertifikats**: Installieren/ersetzen Sie das neue Zertifikat im Central-Überwachungssystem.
- **Neustart der Dienste**: Starten Sie die Dienste des Central-Überwachungssystems neu, um das aktualisierte Zertifikat anzuwenden.
- **Überprüfung der Systemfunktionalität**: Überprüfen Sie das Central-Überwachungssystem, um sicherzustellen, dass die neuen Zertifikate ordnungsgemäß funktionieren.

Für IT-Administratoren in Krankenhäusern ist darüber hinaus die Durchführung der Schlüsselrotation der Software des Central-Überwachungssystems gemäß den Anweisungen in Abschnitt 4.4 (Seite 31) des SDD-SW-031-007 Installationshandbuchs für das Central-Überwachungssystem von entscheidender Bedeutung. Sibel Health benachrichtigt Kunden über den Zeitpunkt der Schlüsselrotation auf der Grundlage des Zeitplans für die Systeminstallation und unter Verwendung einer sicheren E-Mail-Kommunikation.

Sobald die Schlüssel oder Zertifikate erfolgreich im System ersetzt oder rotiert wurden, sollten die IT-Administratoren des Krankenhauses die Funktionalität und den Betrieb des Central-Überwachungssystems überprüfen.

Um die ordnungsgemäße Funktion des Central-Überwachungssystems sicherzustellen, ist Folgendes erforderlich:

- **Validierung durch den IT-Admin über das Administrator-Dashboard**: IT-Administratoren von Krankenhäusern können die Funktionalität der Infrastruktur über das Admin-Dashboard überprüfen, um sicherzustellen, dass alle Dienste betriebsbereit sind. Für die Validierung kann auch ein Überwachungstool verwendet werden, das zur Unterstützung der Ereigniserkennung installiert wurde.
- **Validierung im Administrator-Dashboard**: IT-Administratoren in Krankenhäusern können die grundlegende Funktionalität des Systems überprüfen, indem sie die Benutzerberechtigungen überprüfen und sicherstellen, dass das System seine vorgesehene Funktion korrekt ausführt.

4.1.7.4 Widerruf kryptografischer Assets

Im Falle einer Kompromittierung von Schlüsseln oder Zertifikaten:

- Ungültigkeitserklärung der Schlüssel
- Neuausstellung
- Neukonfiguration

Wenn eine Kompromittierung eines Schlüssels oder Zertifikats festgestellt wird oder die Gültigkeitsdauer oder Cryptoperiod abgelaufen ist, ergreift das IT-/Sicherheitsteam von Sibel Health unverzüglich Maßnahmen: Der betroffene Schlüssel wird für ungültig erklärt, es wird ein neuer Schlüssel ausgestellt und die betroffenen Systeme

werden neu konfiguriert. Darüber hinaus werden die Kunden aufgefordert, unverzüglich Maßnahmen zur Minderung der Sicherheitsrisiken zu ergreifen.

Es ist das in Abschnitt 4.1.7.3„Erstellung und Erneuerung (Rotation) von kryptografischen Assets“ beschriebene Verfahren zu befolgen:

- Kryptographie-Erstellung
- Ungültigkeitserklärung der Schlüssel
- Neuausgabe der Kryptographie
- Ersatz
- Überprüfung des Betriebs

4.1.7.5 Löschung/Vernichtung von kryptografischen Assets

Bei nicht mehr verwendeten kryptografischen Schlüsseln oder Zertifikaten ist der IT-/Sicherheitsmanager von Sibel Health dafür verantwortlich, nicht mehr benötigte kryptografische Assets zu vernichten und aus dem kryptografischen Modul unwiderruflich zu löschen. Dadurch wird jegliche Möglichkeit der Wiederherstellung oder Rekonstruktion der kryptografischen Schlüssel oder sensibler Daten ausgeschlossen. Sibel Health befolgt die Richtlinien aus NIST SP 800-88, welche Standards für die sichere Datenbereinigung festlegen.

Der IT-/Sicherheitsmanager von Sibel Health bestätigt, dass die IT-Administratoren des Kunden dieselben Protokolle befolgen, um die vollständige Löschung der kryptografischen Assets sicherzustellen.

4.2 Außerbetriebnahme (EOL) des Central-Überwachungssystems

4.2.1 Ende der Unterstützung der Version des Central-Überwachungssystems

Versionen des Central-Überwachungssystems werden bis zu zwei Revisionen rückwirkend unterstützt. Sobald eine Revision jedoch nicht mehr unterstützt wird, werden die Kunden über den Upgrade-Pfad zur neuesten Version informiert. Benutzer, die sich gegen Upgrades entscheiden, erhalten keine Updates mehr (weder Sicherheitsupdates noch Patches). Sibel Health wird Kunden Informationen zu bekannten Sicherheitslücken zur Verfügung stellen, um sie über die Risiken zu informieren, die mit der Nichtumstellung auf die neueste Version verbunden sind.

4.2.2 Ende der Lebensdauer des Central-Überwachungssystems

Wenn das Central-Überwachungssystem das Ende seiner Lebensdauer erreicht, wird Sibel Health alle Kunden darüber informieren, ab welchem Datum kein Support mehr angeboten wird und keine zuverlässige Nutzung des Systems mehr zu erwarten ist. Sibel Health hat ein Dokument mit dem Titel „SDD-SW-031-007 Central Monitoring System Installation Manual“ (Installationshandbuch für das Central-Überwachungssystem) erstellt. Darin wird in Abschnitt 6 (Seite 37) beschrieben, wie die Anwendung sicher von ihrem Installationsort entfernt werden kann und welche Optionen für die Datenlöschung zur Verfügung stehen.

Bitte beachten Sie, dass sensible Informationen offengelegt werden können, wenn das System nicht ordnungsgemäß oder unvollständig außer Betrieb genommen wird:

- Vor- und Nachname
- Geburtsdatum
- Patienten-ID

Abschnitt 5. Fehlerbehebung

5.1 Validierung der Verbindung zur Kubernetes-API

Wenn diese Fehlermeldung erscheint,

bedeutet dies, dass die Konfigurationsdatei im Standardverzeichnis „~/.kube“ fehlt. Stellen Sie sicher, dass die Datei vom Installationsverzeichnis in das Standardspeicherverzeichnis kopiert wurde, und versuchen Sie es erneut. Die Datei muss genau konfiguriert sein und sich im Verzeichnis „~/.kube“ befinden.

Um die Kommunikation mit der Kubernetes-Cluster-Datei zu vereinfachen, kann „~/sibel-install/kubeconfig“ in das Verzeichnis „~/.kube“ mit dem Namen „config“ kopiert werden. Dieser Speicherort wird von kubectl standardmäßig überprüft und verwendet.

Die Datei „~/.kube/config“ sollte in etwa wie folgt aussehen:

5.2 Fehler bei der Installation des Central-Überwachungssystems

Während des Installationsvorgangs kann möglicherweise der folgende Fehler oder ein ähnlicher Fehler auftreten:

In den meisten Fällen bedeutet dies, dass der Schritt zur Erstellung von DNS-Einstellungen aus der Installationsanleitung übersprungen wurde. Die DNS-Einträge sind erforderlich, damit die Komponenten des Central-Überwachungssystems miteinander kommunizieren können. Die DNS-Einträge sollten beim DNS-Anbieter für die Domain erstellt werden, die für die Bereitstellung des Central-Überwachungssystems und auch für die Kubernetes-API-Domain verwendet wird.

Für die folgenden Domänen sollten DNS-Einträge erstellt werden:

Als Übergangslösung für die Kubernetes-API-Domäne können Sie die folgende Zeile zur Datei „/etc/hosts“ auf dem Rechner hinzufügen, auf dem die Installation ausgeführt wird:

5.3 Fehlfunktion des Central-Überwachungssystems

Sollte das Central-Überwachungssystem nicht wie erwartet funktionieren, können die folgenden Schritte zur Fehlerbehebung durchgeführt werden:

1. Überprüfen Sie den Status der Komponenten des Central-Überwachungssystems mit dem folgenden Befehl:

Alternativ können Sie diesen Vorgang auch über das Kubernetes-Dashboard durchführen. Melden Sie sich beim Dashboard an, navigieren Sie zum Namespace „central-hub“ und überprüfen Sie den Status der betreffenden Pods auf der Seite „Workloads“.

2. Sollten einzelne Pods nicht den Status „Running“ oder „Completed“ aufweisen, überprüfen Sie bitte die Protokolle dieser Pods, um das Problem zu identifizieren. Die Protokolle können mit folgendem Befehl überprüft werden:

Alternativ können Sie auch das Kubernetes-Dashboard verwenden. Navigieren Sie zum Namespace „central-hub“ und überprüfen Sie die Protokolle der betreffenden Pods auf der Seite „Workloads“.

3. Sollten einige Pods den Status „Pending“ aufweisen, überprüfen Sie die Ereignisse des Pods, um das Problem zu identifizieren. Die Ereignisse können mit folgendem Befehl überprüft werden:

Alternativ können Sie auch das Kubernetes-Dashboard verwenden. Navigieren Sie zum Namespace „central-hub“ und überprüfen Sie die Ereignisse der betreffenden Pods auf der Seite „Workloads“.

Ereignisse sind in der Regel selbsterklärend und können bei der Identifizierung des Problems behilflich sein.

Ein möglicher Grund für die Pods mit dem Status „Pending“ könnte sein, dass der Knoten, auf dem der Pod geplant werden soll, nicht bereit ist oder dass auf dem Knoten nicht genügend Ressourcen vorhanden sind, um den Pod zu planen.

Der Knotenstatus kann mit folgendem Befehl überprüft werden:

Sollte einer der Knoten nicht als „Ready“ angezeigt werden, überprüfen Sie bitte die Ereignisse und den Status des Knotens, um das Problem mithilfe des folgenden Befehls zu identifizieren:

Lesen Sie die Ausgabedaten sorgfältig, um gegebenenfalls Probleme mit dem Knoten zu erkennen.

5.4 Die URL des Central-Überwachungssystems ist nicht erreichbar

Sollte die URL des Central-Überwachungssystems nicht erreichbar sein, können die folgenden Schritte zur Fehlerbehebung durchgeführt werden:

1. Vergewissern Sie sich, dass der DNS-Eintrag für die URL des Central-Überwachungssystems bei Ihrem DNS-Anbieter vorhanden ist. Die korrekte IP-Adresse ist die IP-Adresse des Lastverteilers, der während des Installationsvorgangs erstellt wurde.
2. Wenn der DNS-Eintrag existiert, wäre als Nächstes zu überprüfen, ob der Ingress-Controller im Kubernetes-Cluster ordnungsgemäß funktioniert. Der Ingress-Controller ist dafür zuständig, den Datenverkehr an den richtigen Dienst im Kubernetes-Cluster weiterzuleiten. Verwenden Sie folgenden Befehl, um den Status des Ingress-Controllers zu überprüfen:

Wenn alle Pods den Status „Running“ anzeigen, identifizieren Sie das Problem anhand der Protokolle des Ingress-Controllers mit dem folgenden Befehl:

Der vorstehende Befehl verfolgt die Protokolle der Ingress-Controller-Pods und zeigt die Protokolle in Echtzeit an. Versuchen Sie, eine Verbindung zur URL herzustellen, und überprüfen Sie die Protokolle auf Fehler.

Sie können während der Überprüfung der Protokolle „grep“ verwenden, um den spezifischen Hostnamen zu untersuchen, auf den nicht zugegriffen werden kann, und so das Problem zu identifizieren. Wenn die Protokolle für

den Hostnamen in den Protokollen vorhanden sind, liegt das Problem höchstwahrscheinlich bei den Komponenten des Central-Überwachungssystems, die den Datenverkehr empfangen.

3. Überprüfen Sie, ob der zentrale Hub-Eingang mit Port 443 erstellt wurde, wie unten dargestellt.

4. Sollte dies der Fall sein, überprüfen Sie bitte, ob der geheime Sitzungsschlüssel (central-hub-tls secret) erstellt werden soll.

5. Überprüfen Sie die Protokolle der fehlerhaften Komponenten des Central-Überwachungssystems mit dem folgenden Befehl, um das Problem zu identifizieren:

ANNE View kann keine Verbindung zum Central-Überwachungssystem herstellen.

5.5 ANNE View kann keine Verbindung zum Central-Überwachungssystem herstellen

1. Stellen Sie sicher, dass ANNE View über gültige SDC-Zertifikate verfügt.
2. Vergewissern Sie sich, dass ANNE View und das Central-Überwachungssystem sich im selben Netzwerk befinden.
3. Bitte überprüfen Sie die Protokolle der Fleet-Manager-Pods im Cluster, um eine mögliche Ursache für das Problem zu ermitteln.

Mit dem vorstehenden Befehl werden die Protokolle der SDC-Pods verfolgt und die Protokolle in Echtzeit angezeigt. Versuchen Sie, ANNE View mit dem Central-Überwachungssystem zu verbinden, und überprüfen Sie die Protokolle auf eventuelle Fehler.

5.6 Verbindungsprobleme zwischen den Pods im Cluster, wenn die Pods auf verschiedenen Knoten ausgeführt werden

1. Der Kubernetes-Cluster verwendet das Overlay-Netzwerk, um die auf verschiedenen Knoten ausgeführten Pods miteinander zu verbinden. Das Overlay-Netzwerk wird durch das auf dem Cluster installierte CNI-Plugin erstellt. Das CNI-Plugin ist für die Erstellung des Netzwerks und die Verwaltung des Netzwerkverkehrs zwischen den Pods zuständig.
2. Falls die Pods nicht miteinander kommunizieren können, überprüfen Sie zunächst den Status der Knoten mit folgendem Befehl:

3. Wenn die Knoten den Status „Ready“ anzeigen, überprüfen Sie den Status der CNI-Pods mit folgendem Befehl:

Wenn die Pods nicht den Status „Running“ anzeigen, überprüfen Sie bitte die Protokolle des Pods mit dem folgenden Befehl, um das Problem zu bestimmen:

5.7 Änderung der Cluster-IP-Adressen nach dem Neustart des Servers

WARNUNG: Es sollten Vorsichtsmaßnahmen getroffen werden, um zu verhindern, dass sich die IP-Adressen der Knoten im Kubernetes-Cluster nach dem Neustart des Servers ändern. Stellen Sie sicher, dass die den Kubernetes-Clusterknoten zugewiesenen IP-Adressen statisch sind und nicht vom DHCP-Server im Netzwerk zugewiesen werden.

Sollten sich die IP-Adressen der Knoten im Kubernetes-Cluster nach dem Neustart des Servers ändern, ist es erforderlich, den Kubernetes-Cluster mit den neuen IP-Adressen zurückzusetzen. Führen Sie die folgenden Schritte aus, um den Kubernetes-Cluster mit den neuen IP-Adressen zurückzusetzen:

1. Stellen Sie über SSH eine Verbindung zum Control-Plane-Knoten des Kubernetes-Clusters her.
2. Erstellen Sie das Verzeichnis „k3s_backup“.
3. Kopieren Sie die k3s-Binärdatei und das Installationsskript in das Verzeichnis „k3s_backup“
4. Halten Sie den K3S-Dienst an.
5. Entfernen Sie zunächst „k3s“, indem Sie das folgende Skript ausführen.

`k3s-killall.sh`

6. Installieren Sie nun „k3s“ mit der neuen 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. Überprüfen Sie den Status der Clusterknoten.

Abschnitt 6. Offenlegung von Sicherheitslücken

6.1 Sibel-Richtlinie zur Offenlegung von Sicherheitslücken

Als Anbieter von sicherer Software, Dienstleistungen und Rechercheleistungen nimmt das Personal des Kundensupports Sicherheitsfragen ernst und ist sich der Bedeutung von Datenschutz, Sicherheit und öffentlicher Aufklärung bewusst. In diesem Sinne ist das Personal des Kundensupports dazu verpflichtet, Sicherheitsprobleme aufzugreifen und zu melden. In dieser Richtlinie wird beschrieben, wie Sicherheitslücken gemeldet werden können, welche Reaktion zu erwarten ist und wie das Personal des Kundensupports damit umgeht.

6.2 Meldung von Sicherheitsproblemen

Wenn Sie der Ansicht sind, eine Schwachstelle in einem Produkt entdeckt zu haben, oder ein Sicherheitsproblem melden möchten, gehen Sie bitte wie folgt vor:

- **E-Mail**: Senden Sie einen detaillierten Bericht an security@sibelhealth.com. Sollten Sie eine Verschlüsselung für erforderlich halten, nutzen Sie bitte unseren unten angegebenen öffentlichen PGP-Schlüssel, um Ihre Kommunikation mit uns zu verschlüsseln.
    - Öffentlicher PGP-Schlüssel
- **Geben Sie bitte die folgenden Informationen an:**
    - Eine detaillierte Beschreibung der Sicherheitslücke, einschließlich
        - Produkt- oder Dienstname, URL und betroffene Versionen.
        - Betriebssystem der beteiligten Komponenten.
        - Softwarekonfiguration des Computers oder Geräts zum Zeitpunkt der Entdeckung der Sicherheitslücke.
        - Klasse oder Art der Sicherheitslücke (z. B. unter Verwendung einer Taxonomie wie CWE).
        - Zeitpunkt und Datum der Entdeckung.
    - Schritte zur Nachstellung des Problems
        - Technische Beschreibung, Reihenfolge und Ergebnisse der durchgeführten Maßnahmen.
        - PoC-Code/Tools, die zur Erzeugung des sicherheitsrelevanten Verhaltens verwendet wurden.
    - Abschätzung der potenziellen Auswirkungen und des Schweregrades, sofern verfügbar.
    - Mögliche Ursache, falls verfügbar.
    - Einschätzung des Umfangs, andere Produkte, Komponenten, Dienstleistungen oder Anbieter, von denen angenommen wird, dass sie betroffen sind, sofern verfügbar.
    - Offenlegungspläne, insbesondere Sperrfristen und Veröffentlichungszeitpläne, sofern verfügbar.

6.3 Unsere Verpflichtung

Wenn dem Kundensupport eine Sicherheitslücke gemeldet wird, verpflichten wir uns:

- Den Eingang Ihrer Meldung innerhalb von 7 Werktagen zu bestätigen.
- Die Legitimität der Sicherheitslücke zu prüfen und zu verifizieren.

- Den Schweregrad der Sicherheitslücke auf der Grundlage ihrer potenziellen Auswirkungen zu kategorisieren.
- Einen Fehlerbehebungsplan auf Grundlage des Schweregrads zu entwickeln und eine Lösung zu implementieren.
- Einen geschätzten Zeitrahmen für die Fehlerbehebungsmaßnahmen anzugeben.
- Sie während des gesamten Fehlerbehebungsprozesses per E-Mail auf dem Laufenden zu halten.
- Sie gemäß unserem internen Verfahren zum Management von Sicherheitslücken beratend zu unterstützen.
- Jede Meldung vertraulich zu behandeln und nicht ohne Zustimmung an Dritte weiterzugeben.
- Sicherheitslücken in den Versionshinweisen der Updates offenzulegen.

Bitte beachten Sie, dass nicht alle Probleme in den Geltungsbereich des Verfahrens zur Offenlegung von Sicherheitslücken seitens der Firma Sibel fallen. Dazu gehören unter anderem:

- Meldungen zu fehlenden Sicherheitsheadern, die keine wesentlichen Auswirkungen oder Leistungseinbußen zur Folge haben.
- Nicht mehr relevante plattformspezifische Probleme.
- Social-Engineering-Angriffe oder physische Schwachstellen (z. B. Bürosicherheit).
- Probleme mit Drittanbieterdiensten, die nicht vom Kundensupport-Verantwortlichen verwaltet werden

Abschnitt 7. Anhang

7.1 Maschinenlesbares 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