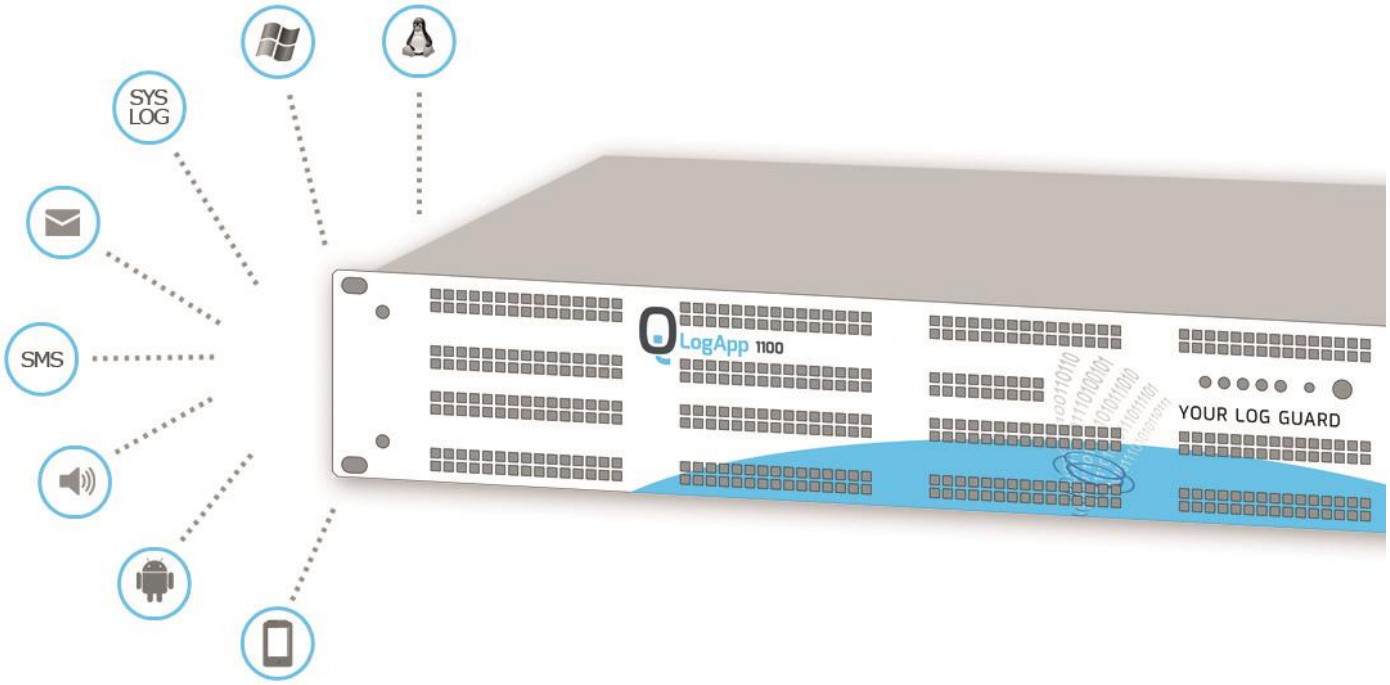

LogApp Benutzerhandbuch

Version 4.2

13. Dezember 2024

Inhaltsverzeichnis

1 Komponenten

Die LogApp Systemlandschaft besteht aus folgenden Komponenten:

- LogApp (Hardware) oder LogApp VM (virtuelle, basierend auf VMware oder Hyper-V)
    - Zentrale Appliance zum Management aller Komponenten, Sammeln von Logs, regelbasiertem Alarmieren sowie langfristigem Archivieren der Logs
    - Lokale Netzwerk-Schnittstelle zur direkten Anbindung von Netzwerk-Quellen
- LogAgents (Windows ab Server 2012, Linux) mit integriertem Netzwerk-Proxy
- Enterprise Reporting Server basierend auf
    - MS SQL Server ab Version 2008 inkl. Server Reporting Services

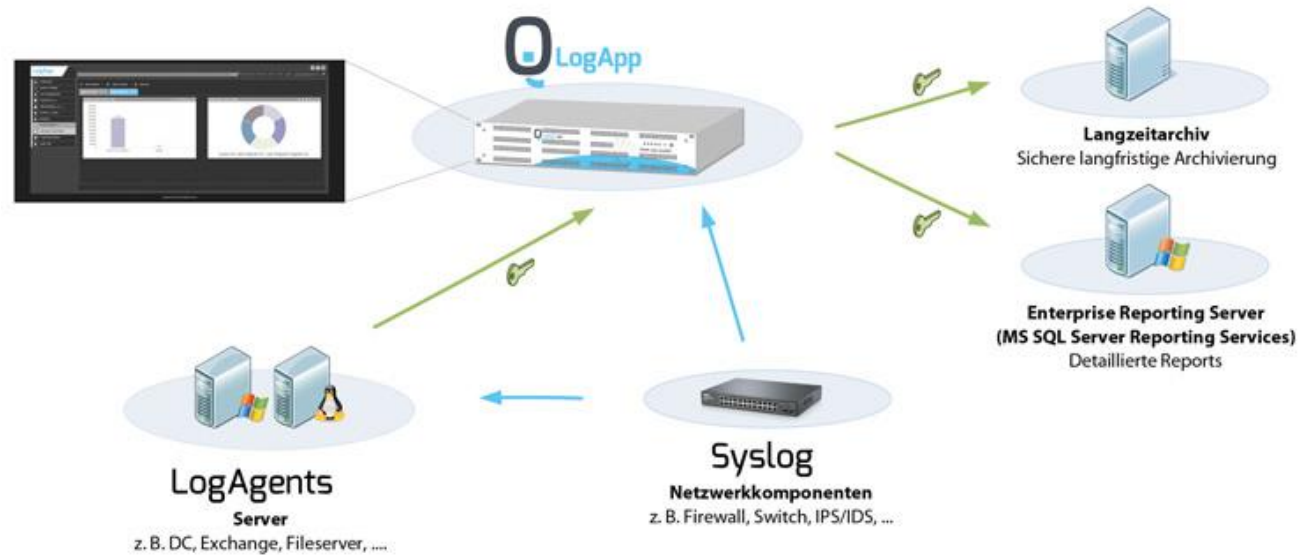

Abbildung 1: LogApp Komponenten

2 Installation

2.1 Vorbereitungen

2.1.1 Netzwerkverbindungen

Die LogApp wird standardmäßig mit einer Netzwerkschnittstelle betrieben. Sowohl das WebInterface, als auch die Schnittstellen für die LogAgents sind über dieses zu erreichen.

Es gibt auch die Möglichkeit, mehrere Interfaces zu konfigurieren sollte es notwendig sein und zum Beispiel ein eigenes Management und ein eigenes Servernetzwerk vorliegen.

Bei LogAgents entscheiden die lokal eingetragenen Routen, welches Interface für die Kommunikation zur LogApp verwendet wird. Syslog-fähige Geräte (z.B. Firewalls oder Switches) können Syslog Nachrichten an einen beliebigen LogAgent senden. Für kleinere Umgebungen bietet sich der Lokale NetworkProxy der LogApp an. Netzwerkgeräte können auch an diesen senden.

2.1.2 Benötigte Ports

Folgende Ports werden für eine ordnungsgemäße Kommunikation benötigt:

Zweck	Richtung			Port
LogApp ausgehende Kommunikation				
Mail	LogApp	⇨	Mailserver	25/TCP
Alarmierung	LogApp	⇨	AMS[1]	4656/TCP
LDAP(S)	LogApp	⇨	LDAP	389/TCP (LDAP) 636/TCP (LDAPS)
DNS	LogApp	⇨	DNS	53/UDP
Langzeitarchivierung	LogApp	⇨	CIFS	445
Radius	LogApp ⇨	Radius.		1812/UDP 1813/UDP
LogApp eingehende Kommunikation				
LogAgent Heartbeat und Zertifikatsaustausch	LogAgent	⇨	LogApp	1735/TCP
LogAgent Eventkommunikation	LogAgent	⇨	LogApp	1737/TCP
LogAgent File Integrity Service	LogAgent	⇨	LogApp	1738/TCP
Enterprise Reporting Server	ERS	⇨	LogApp	3306/TCP
LogApp Analysis Interface	Analysis Interface	⇨	LogApp	9400/TCP
System Monitoring (SNMP)	Monitoring	⇨	LogApp	161/UDP

Tabelle 1: Benötigte Kommunikationsports

2.2 Komponenten

Die zentrale Log-Appliance LogApp kann jeweils als Hardware Appliance oder als virtuelle Maschine betrieben werden. Die Betriebsvarianten sind beliebig kombinierbar. Die Installation der LogAgents erfolgt manuell am Host.

Die Installation der jeweiligen Auslieferungsoption wird in den folgenden Abschnitten beschrieben.

[1] Alert Messaging Server (AMS): dient zur erweiterten Alarmierung auch über SMS und Voice.

2.3 LogApp VM - Vorbereitungen

Für diese Art der Installation muss eine virtuelle Maschine mit folgenden Mindestsystemanforderungen vorbereitet werden:

- min. 4 Cores
- min. 8 GB RAM
- min. 250 GB HDD
- 1-2 Ethernet Interfaces

Das genaue Sizing (CPU, RAM, HDD) ist abhängig vom geschätzten Datenaufkommen pro Sekunde (v.a. CPU, RAM) und von den geplanten Aufbewahrungsfristen (v.a. HDD)!

Für das erste Netzwerkinterface wird während der Installation eine statische IP-Adresse vergeben. Nach der Installation ist unter dieser IP-Adresse das Web-Interface verfügbar.

Hinweise für VMware

Geben Sie als Betriebssystem Ubuntu Server 64-Bit an, wenn Sie während des Anlegens einer neuen virtuellen Maschine in VMware danach gefragt werden.

2.4 Grundinstallation

Wird die LogApp von einem Installationmedium aus gestartet, so erscheint folgender Screen.

Abbildung 2: Start der Installation

Hier ist zwar eine Eingabe möglich aber nicht nötig. Die LogApp beginnt automatisch mit der Installation und der ersten Systemeinrichtung.

Ist dies Abgeschlossen, so erscheint ein Wizzard, welcher die Netzwerkeinstellungen abfrägt und die Lokalisierung.

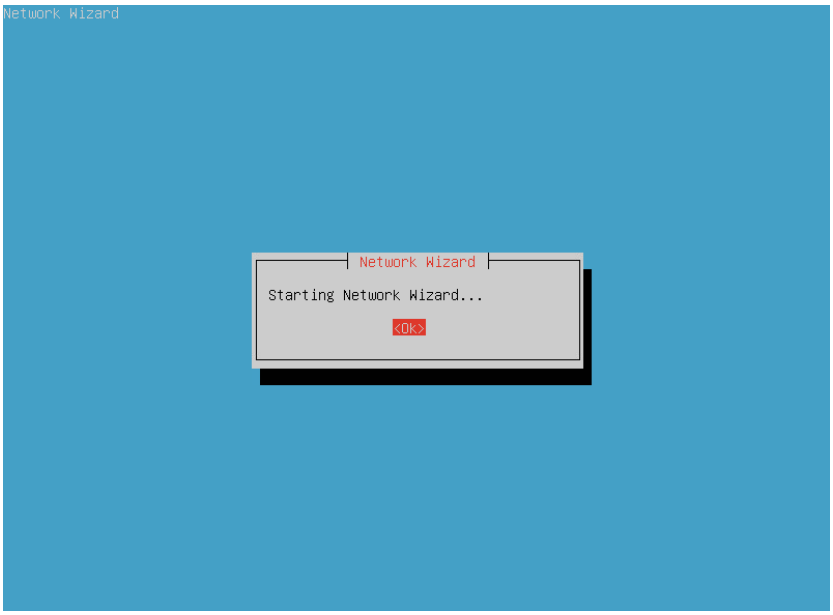

Abbildung 3: Installationsmenü

Nach dem Abschluss des Wizzards ist das Grundsetup der LogApp vollständig durchlaufen und es kann mit dem Web Setup Wizard begonnen werden.

2.5 Web Setup Wizard

Nachdem die LogApp-Installation abgeschlossen ist, können Sie sich über die während der Installation konfigurierte IP-Adresse mit einem Webbrowser auf das Management-Interface verbinden. Geben Sie dazu einfach die IP in der Adressleiste des Browsers ein. Sie werden automatisch auf eine sichere HTTPS-Verbindung umgeleitet. Beim ersten Verbinden muss die Zertifikatswarnung akzeptiert werden.

Bei dem ersten Zugriff auf die WEB GUI wird der Installations-Wizard gestartet. Auf der ersten Seite des Wizards erscheint die Sprachauswahl, wobei zwischen Deutsch und Englisch gewählt werden kann.

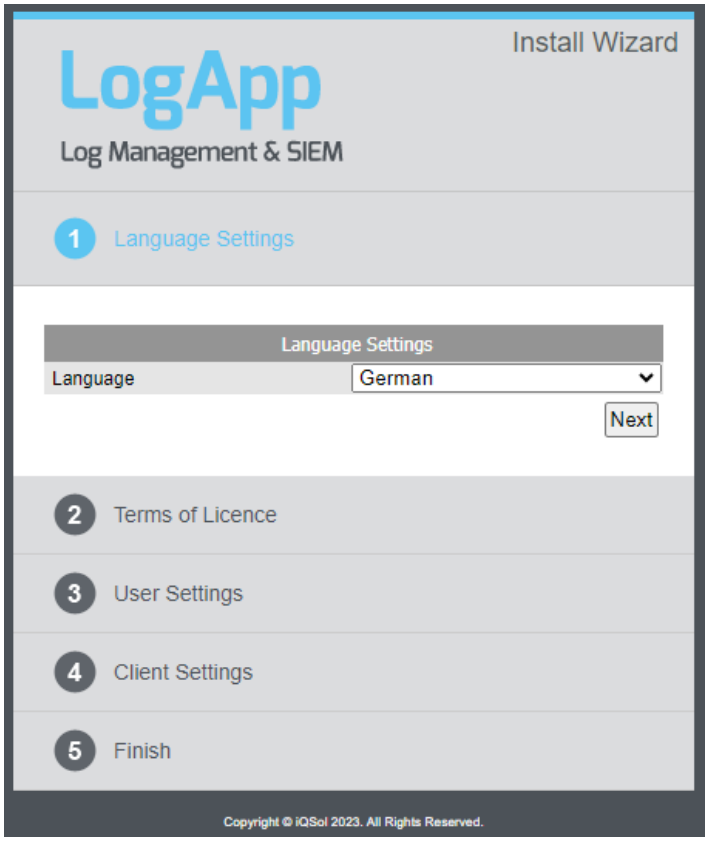

Abbildung 4: Sprachauswahl

Im nächsten Schritt müssen die LogApp Lizenzbedingungen akzeptiert werden, um mit der Installation fortzufahren.

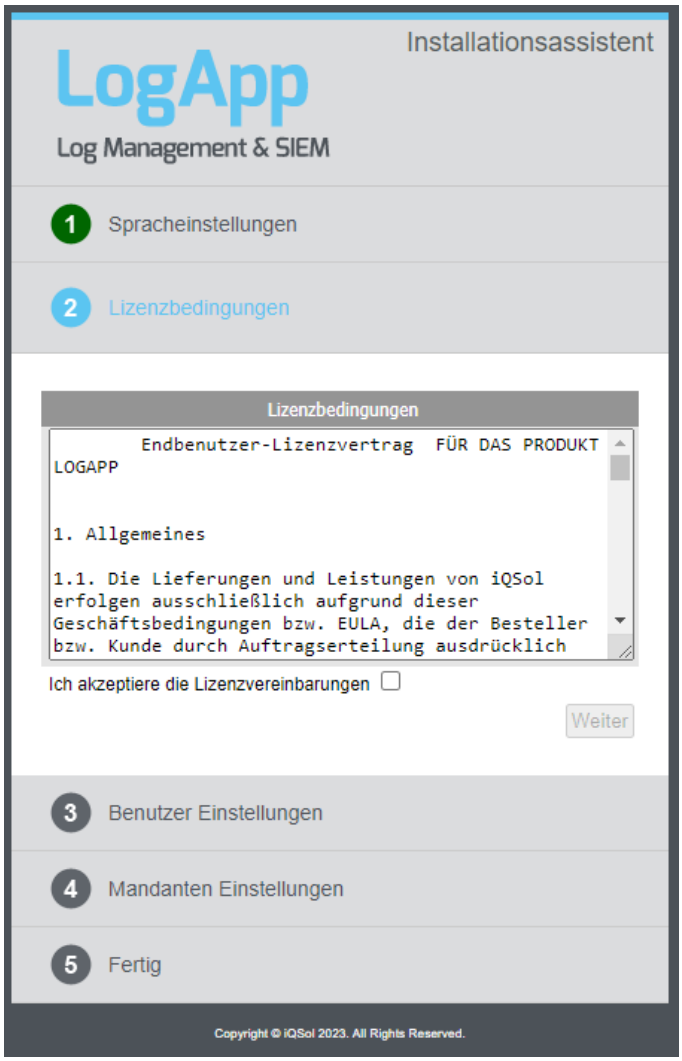

Abbildung 5: Lizenzbedingungen

In Schritt 3 muss das Passwort für den Superadmin-Account geändert werden. Legen Sie ein neues, sicheres Passwort fest. Das Passwort muss Kleinbuchstaben/Großbuchstaben sowie Zahlen beinhalten. Folgende Zeichen dürfen nicht im Passwort enthalten sein: ä, Ä, ö, Ö, ü, Ü, §, €, ß.

Zusätzlich muss eine E-Mail-Adresse für Benachrichtigungen an den Superadmin festgelegt werden.

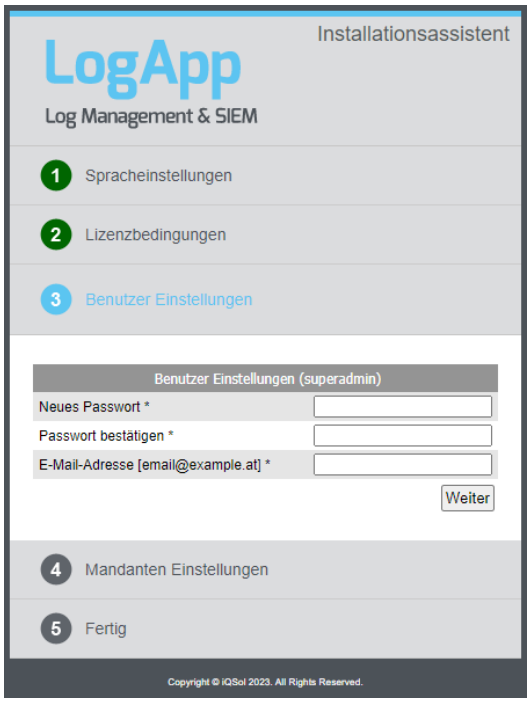

Abbildung 6: Passwortänderung

Im letzten Schritt wird ein Mandant angelegt und das Passwort für den Admin-Account dieses Mandanten vergeben. Hierfür gelten die gleichen Kriterien wie im Schritt zuvor.

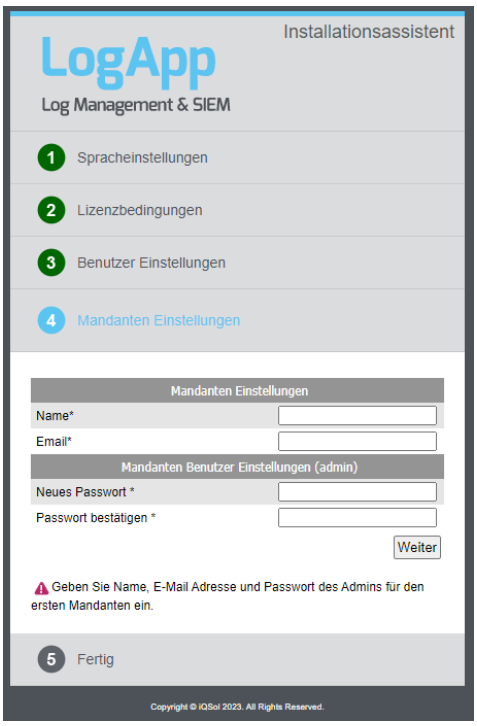

Abbildung 7: Mandanteneinstellungen

Nach dem Anlegen eines Mandanten ist der Setup Wizard abgeschlossen. Durch einen Klick auf den grünen Haken gelangen Sie zum Superadmin Dashboard.

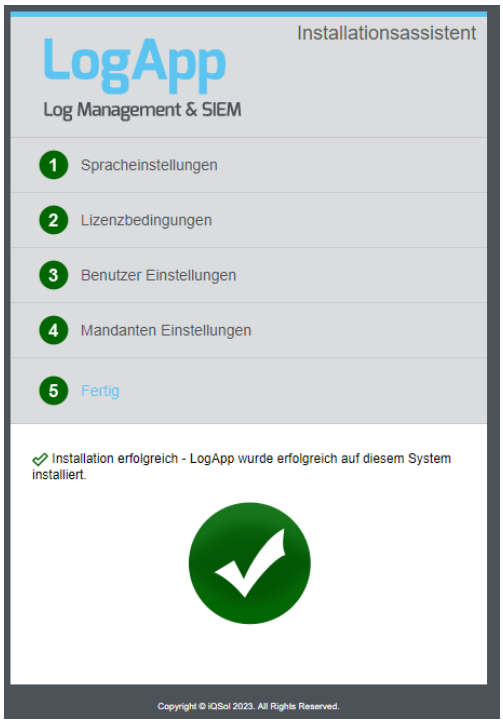

Abbildung 8: Setup Wizard abgeschlossen

3 Erste Schritte

3.1 Login

Nachdem der LogApp-Setup-Wizard abgeschlossen ist, können Sie sich über das Management-Interface anmelden.

Es gibt zwei Anmeldemöglichkeiten:

- Mit dem Benutzernamen „Superadmin“ und dessen Passwort können Sie sich an der mandantenunabhängigen Zentralkonsole anmelden.
- Mit Benutzername, Passwort und Mandantenname können Sie sich an einem konfigurierten Mandanten anmelden.

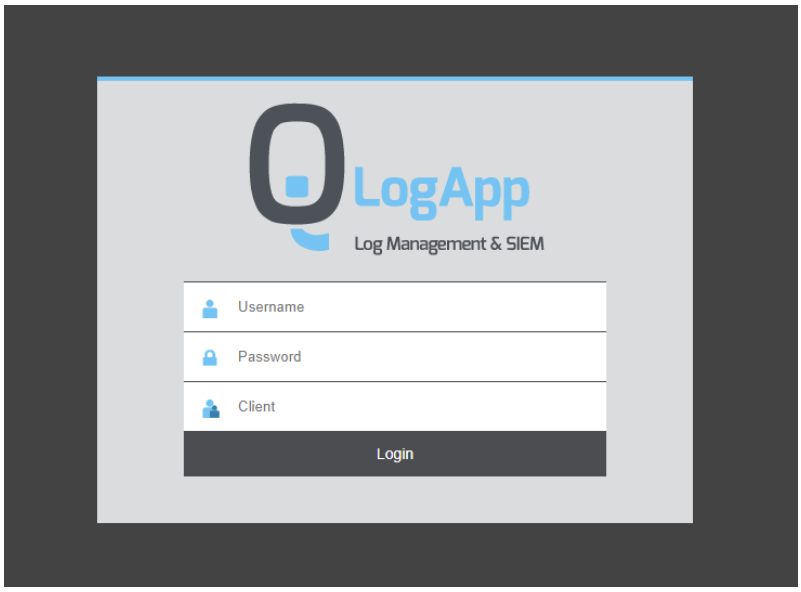

Abbildung 9: LogApp Login

Wird zur Anmeldung ein LDAP-Benutzer verwendet, so ist dieser ohne den Domänennamen anzugeben. Ein Benutzer „exampledomain\Administrator“ wird sich nicht anmelden können, obwohl er hinzugefügt wurde. Die erfolgreiche Anmeldung gelingt mit „Administrator“.

3.2 Aufbau der Weboberfläche

Nach der Anmeldung erscheint das Dashboard. Hier wird eine Übersicht, über die wichtigsten Systeminformationen in Form von Widgets gegeben. Die Widgets können durch Drag & Drop frei angeordnet werden. Genauere Informationen zum Dashboard finden Sie im Kapitel 5.1.

Auf der linken Seite der LogApp GUI befindet sich das Menü. Durch Klick auf einen Menüpunkt erscheinen die Unterpunkte, sofern vorhanden. Andernfalls wird der Inhalt im rechten Teil des Fensters angezeigt.

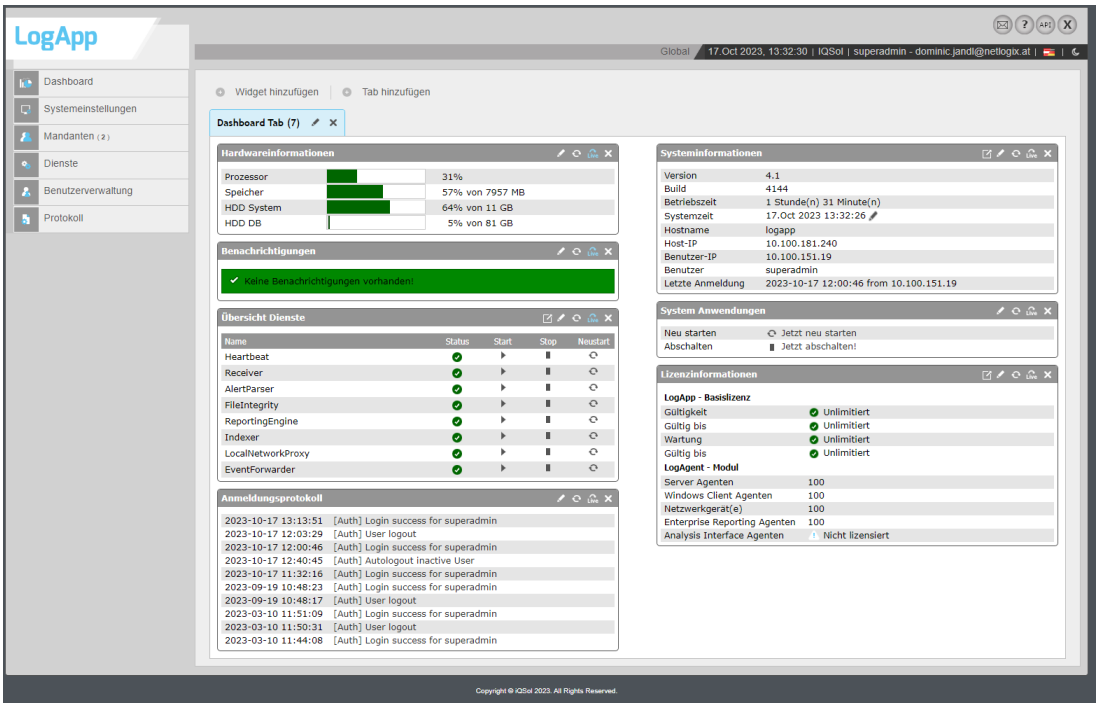

Abbildung 10: LogApp Web GUI

Zu jeder Seite der Weboberfläche sind Hilfetexte vorhanden, ausgenommen dem Dashboard. Diese werden durch einen Klick auf „Info“ im unteren Teil der Seite angezeigt.

Die Weboberfläche ist in die zwei Bereiche, Zentralkonsole und Mandantenkonsole, geteilt. In der Zentralkonsole, erkennbar an der Überschrift „Global“ neben dem Datum und der Uhrzeit, können Einstellungen vorgenommen werden, die alle Mandanten betreffen, beispielsweise das Installieren von Updates oder das Wiederherstellen von Backups. Darüber hinaus werden in der Zentralkonsole Mandanten angelegt und Lizenzen verwaltet.

In der Mandantenkonsole, mit der Überschrift „Client“, erfolgt die Verwaltung von LogAgents sowie das Bearbeiten von Ereignissen und Alarmen mit dem dazugehörigen Regelwerk.

3.3 Mandanten anlegen und Lizenzen zuteilen

Der erste Mandant wird während des Setup Wizards angelegt. Diesem Mandanten werden automatisch alle Demo - Lizenzen zugewiesen.

Um die Aufteilung der Lizenzen einzusehen klicken Sie im Menü auf „Systemeinstellungen“ -> „Lizenz“.

Standardmäßig ist auf der LogApp eine 30 Tage Demo Lizenz vorinstalliert. Danach ist der Upload einer produktiven Lizenzdatei auf dieser Seite notwendig.

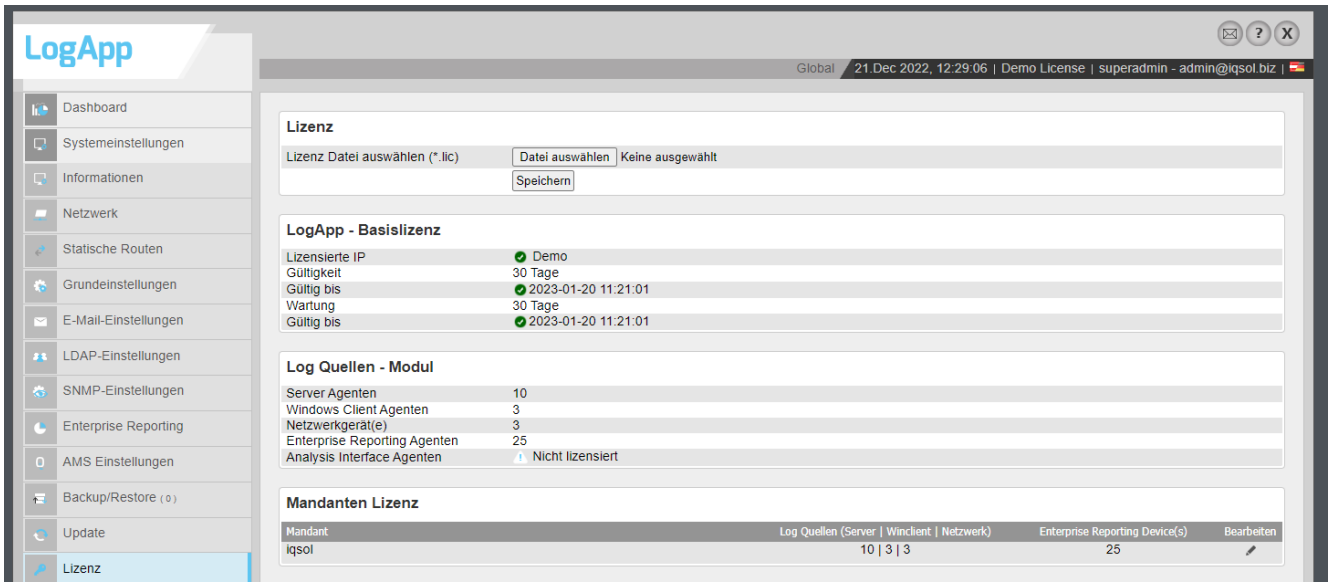

Abbildung 11: Lizenzverwaltung

Im unteren Teil der Seite können die Lizenzen für LogAgents auf die Mandanten verteilt werden. LogAgents können von den entsprechenden Mandanten nur eingesetzt werden, wenn Lizenzen dafür vorhanden sind.

Abbildung 12: Verteilung der Lizenzen

Basis- und Wartungslizenzen gelten für das gesamte Produkt und müssen nicht auf Mandanten verteilt werden.

Genauere Informationen über Lizenzen erhalten Sie im Kapitel 5.2.11.

3.4 E-Mail-Einstellungen konfigurieren

E-Mail-Einstellungen für Benachrichtigungen bei systemrelevanten Notfällen (z.B. Festplatte voll) oder bei Alarmen von LogAgents müssen in der Zentralkonsole und in der Mandantenkonsole voneinander unabhängig konfiguriert werden. Die Einstellungen sind jeweils unter „Systemeinstellungen“ -> „E-Mail-Einstellungen“ zu finden. Mit dem Button „Testmail senden“ können die Einstellungen überprüft werden.

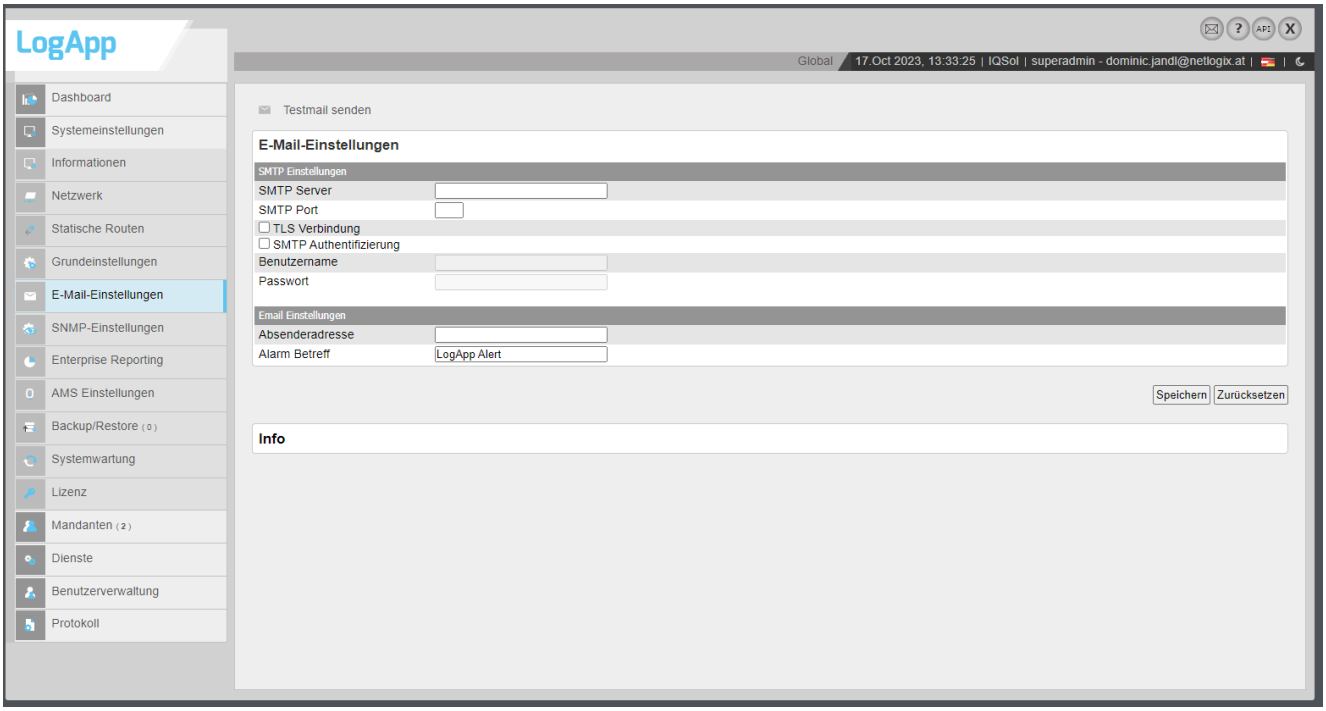

Abbildung 13: E-Mail-Einstellungen

3.5 LogAgents verwalten

LogAgents werden in der Mandantenkonsole im Menüpunkt „Log Quellen“ -> „LogAgents“ verwaltet.

Die LogAgents werden über eigene Installationspakete installiert. Diese können über den Button LogAgent herunterladen heruntergeladen werden.

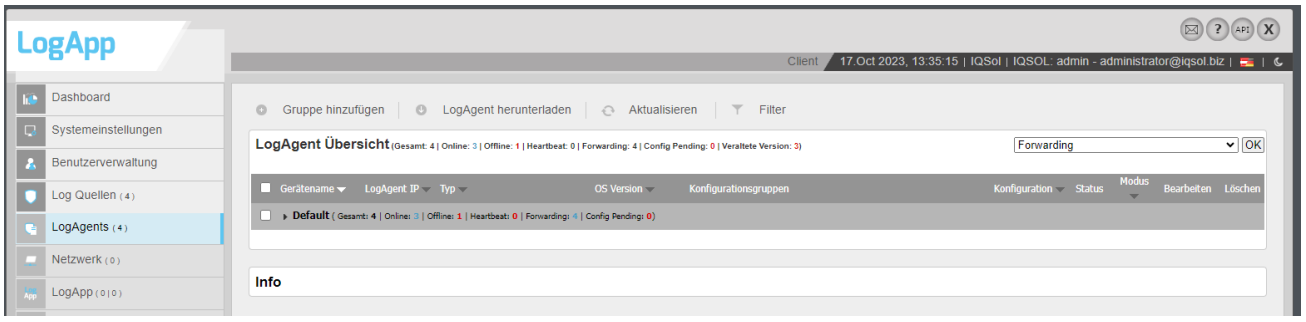

Abbildung 14: LogAgent Übersicht

Nach der Installation werden die LogAgents in der LogAgent Übersicht angezeigt. Standardmäßig wird eine Self-Monitoring Konfigurationsgruppe zugewiesen und der LogAgent läuft im Heartbeat-Modus, dabei werden noch keine Events gesendet.

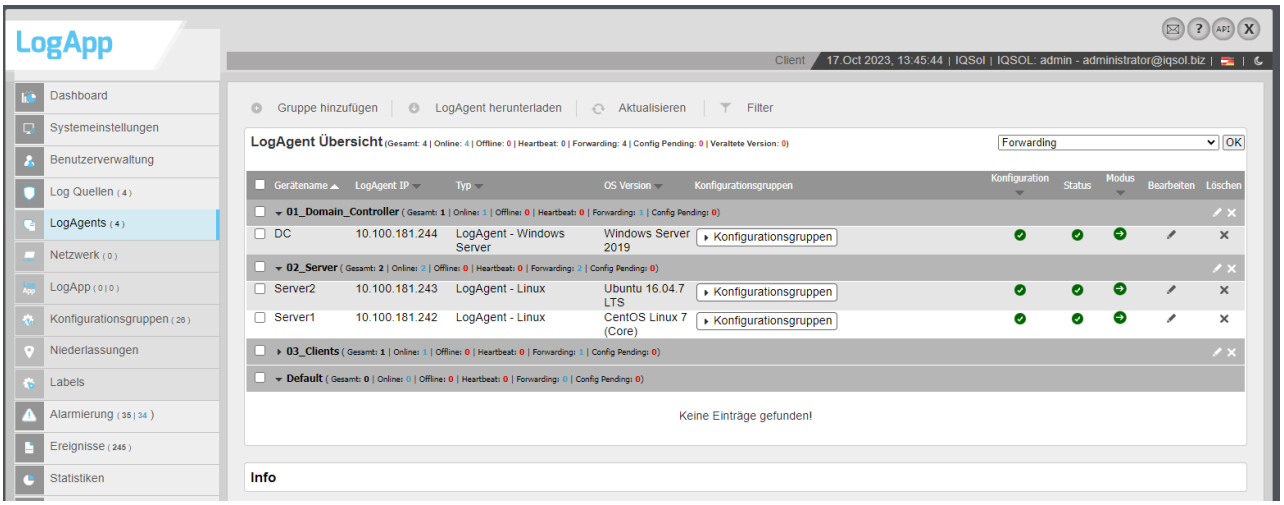

Abbildung 15: LogAgent Übersicht

Durch einen Klick auf das Symbol in der Spalte Modus kann der LogAgent in den Forwarding - Modus geschaltet werden, sodass Events gesendet werden.

Welche Events der LogAgent sendet, wird über die Zuweisung von Konfigurationsgruppen gesteuert. Die genauen LogAgent-Einstellungen können im Bearbeiten-Menü verändert werden.

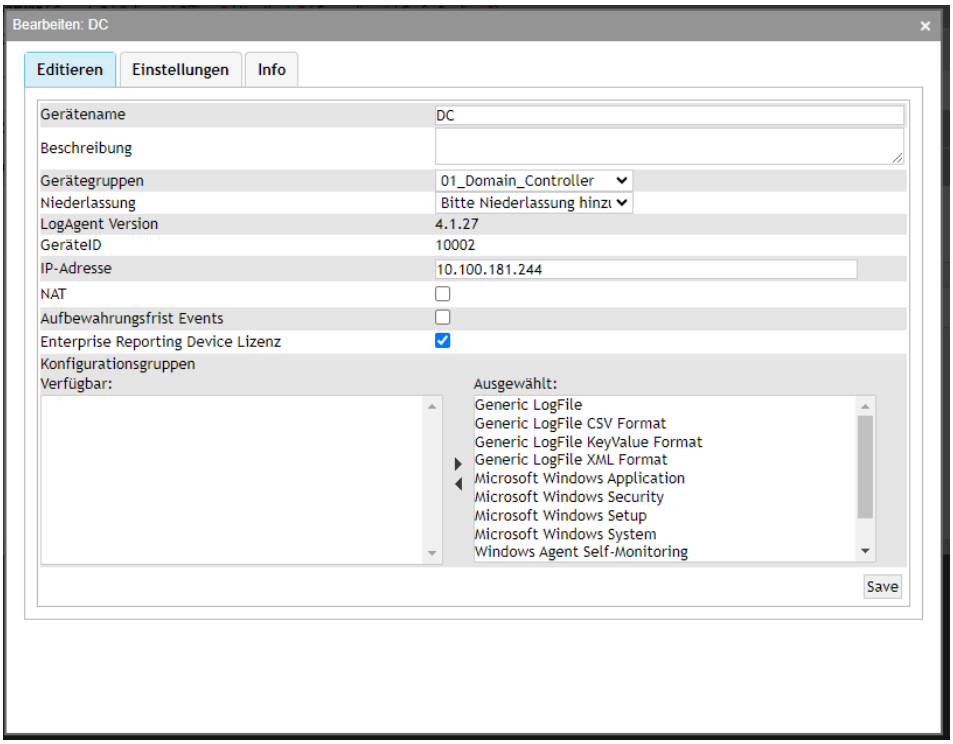

Abbildung 16: LogAgent-Einstellungen bearbeiten

Durch das Zuweisen von Konfigurationsgruppen sendet der LogAgent Events aus den entsprechenden Log-Quellen an die LogApp.

Konfigurationsgruppen können unter „Log Quellen“ -> „Konfigurationsgruppen“ eingesehen, angelegt und geändert werden. Zugewiesene Konfigurationsgruppen werden in der LogAgent Übersicht angezeigt.

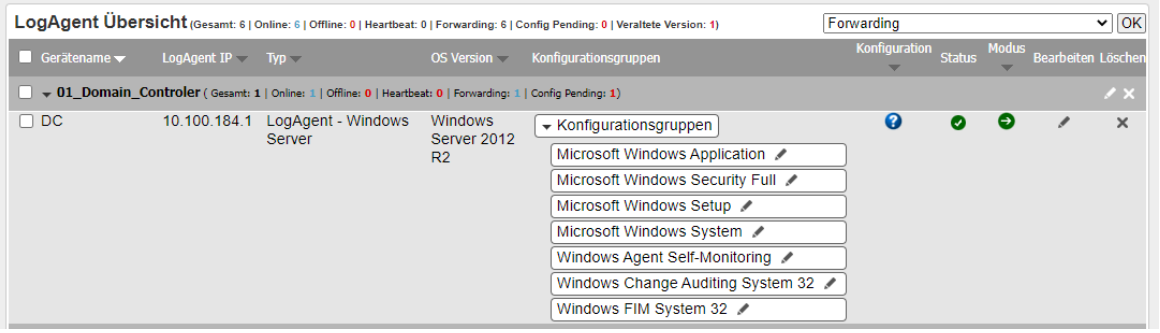

Abbildung 17: Konfigurierte LogAgents

Ein blaues Fragezeichen in der Spalte „Konfiguration“ zeigt an, dass eine geänderte Konfiguration noch nicht zum LogAgent übermittelt wurde. Durch einen Klick auf dieses Symbol löst man nach einer Bestätigungsabfrage die Übertragung aus. In der Zeit zwischen dem Bestätigen und der erfolgreichen Übertragung erscheint ein Warndreieck, welches verschwindet, wenn der Agent seine Konfiguration erhalten hat.

Ist das Icon in der Spalte „Konfiguration“ grün, so kann mit Klick auf dieses ein Neustart des LogAgent forciert werden.

Die Spalte Status gibt den Status des LogAgents an. Hier können 4 verschiedene Status vorkommen.

Status	Symbol	Erklärung
Online		Der Agent liefert regelmäßige Heartbeats und verwendet die neueste Version des LogAgents.
Offline		Der Agent liefert keine Heartbeats mehr, verwendet aber die neueste Version des LogAgents.
Veraltet (online)		Dieser Agent verwendet eine veraltete Version und sollte upgedated werden. Der Agent liefert allerdings noch immer Heartbeats.
Veraltet (offline)		Dieser Agent verwendet eine veraltete Version und sollte upgedated werden. Allerdings liefert dieser Agent auch keine Heartbeats mehr.

Tabelle 2 : LogAgent Status

Die genaue AgentVersion kann beim Bearabeiten des LogAgents eingesehen werden.

3.6 Events und Alarme anzeigen

Sobald LogAgents konfiguriert wurden, werden eingehende Events im Menü unter „Ereignisse“ angezeigt.

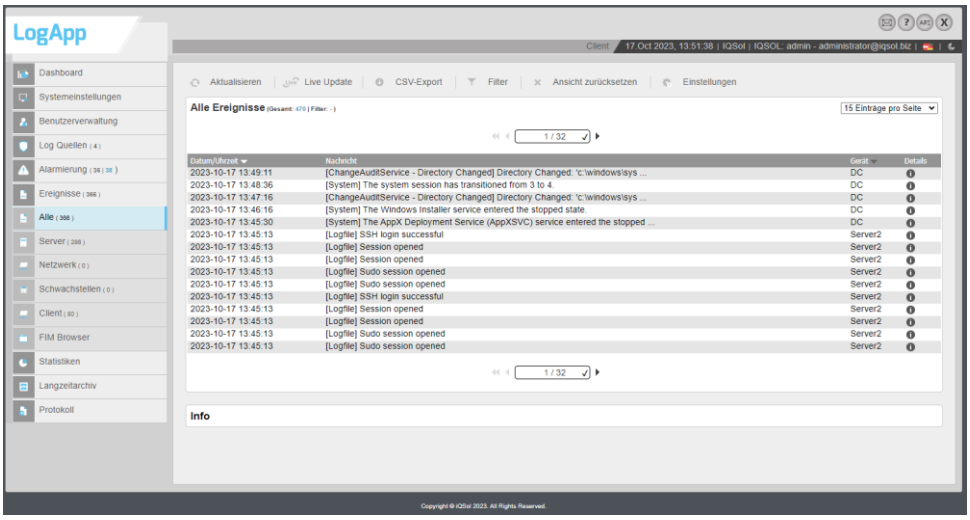

Abbildung 18: Events

Über die Menüpunkte kann unterschieden werden, ob alle Events, Server Events, Netzwerk Events (Syslog), Events von Schwachstellen-Events, Events von WindowsclientAgent und der FIM Browser angezeigt werden sollen.

Durch einen Klick auf den „Filter“-Button im oberen Bereich kann das Anzeigeergebnis weiter eingeschränkt werden.

Durch einen Klick auf den „Details“-Button können einzelne Events eingesehen werden.

Genauere Informationen über den Menüpunkt „Ereignisse“ erfahren Sie in Kapitel 7.

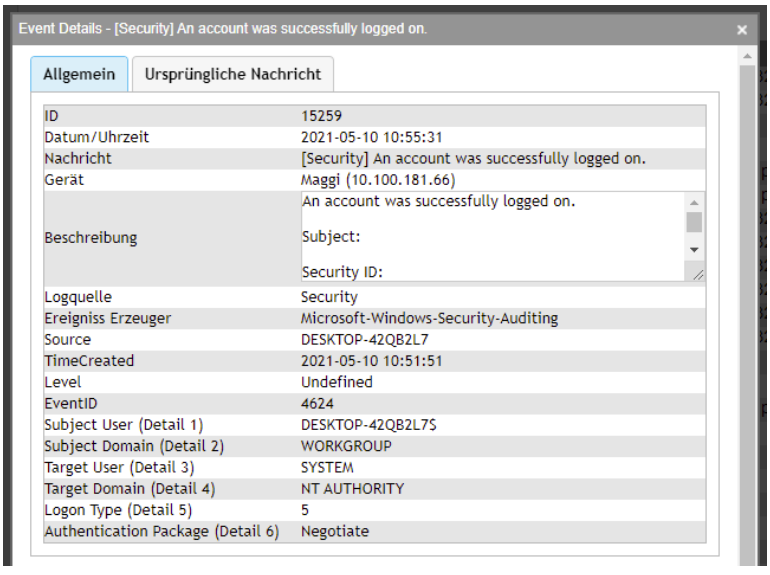

Abbildung 19: Event Details

Alle eingehenden Events werden vom Alert Parser-Service gegen ein hinterlegtes Regelwerk hinsichtlich sicherheitsrelevanter Ereignisse geprüft. Kommt es zu einem Treffer, wird ein Alarm generiert. Alarme können im Menü unter „Alarmierung“ -> „Alarme“ eingesehen werden.

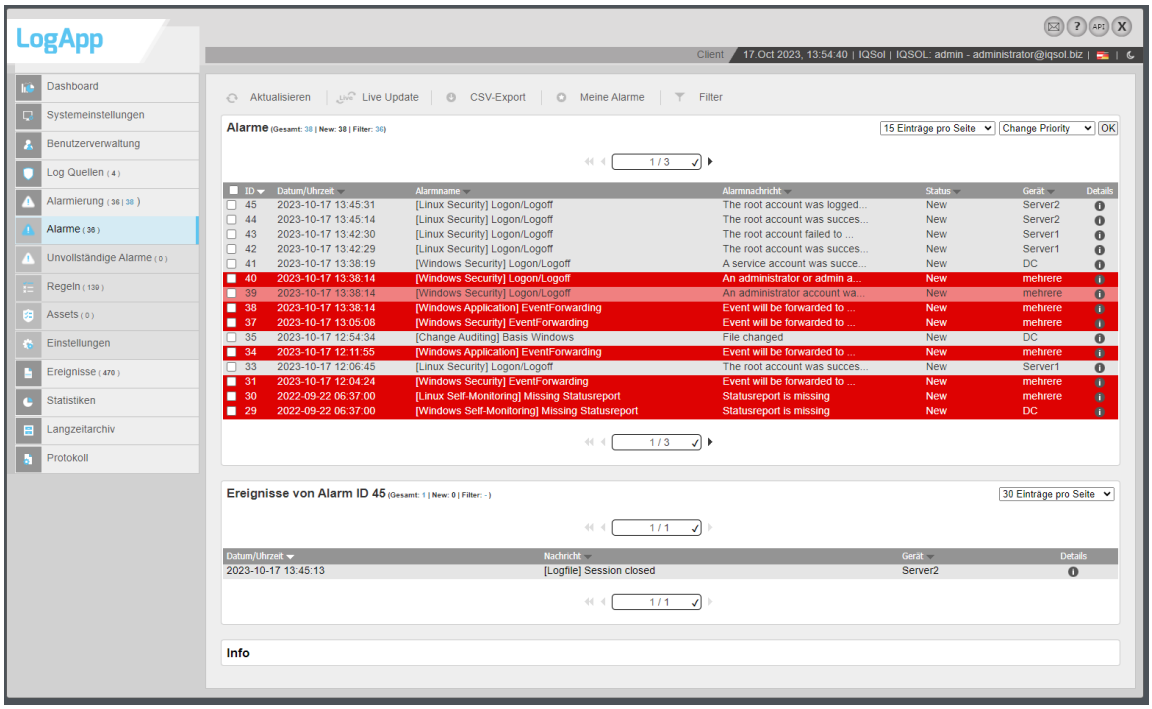

Abbildung 20: Alarm-Übersicht

Alarme werden im oberen Teil der Seite farblich codiert für die Priorität angezeigt. Durch einen Klick auf einen Eintrag werden in der unteren Liste die Events angezeigt, die den Alarm verursacht haben. Die anderen Alarme werden dabei grau hinterlegt.

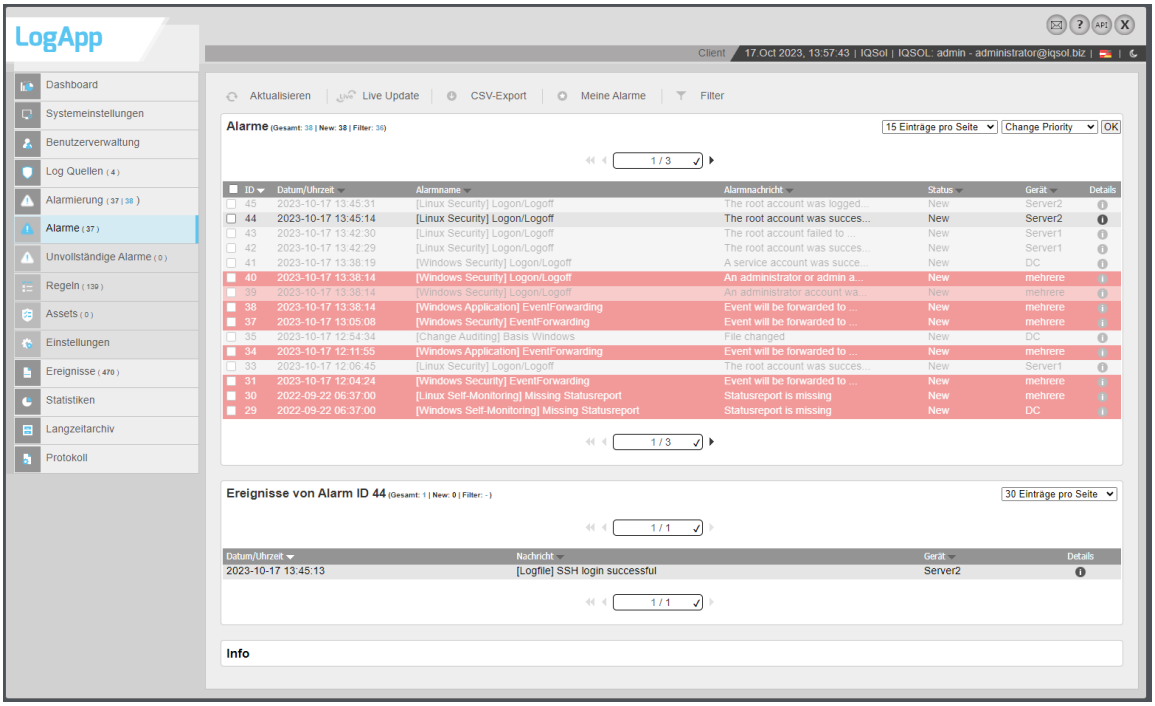

Abbildung 21: ausgewählter Alarm mit dazugehörigen Events

Auch für Alarme stehen Filtermöglichkeiten zur Verfügung, die über den „Filter“-Button am oberen Rand der Seite konfiguriert werden.

Durch einen Klick auf den „Details“-Button in der Alarmliste können Alarmdetails bearbeitet werden. Alarme können Benutzern zugewiesen werden, die dann eine Benachrichtigung per E-Mail erhalten. Status und Priorität können bearbeitet werden und Kommentare zu Alarmen können vergeben werden.

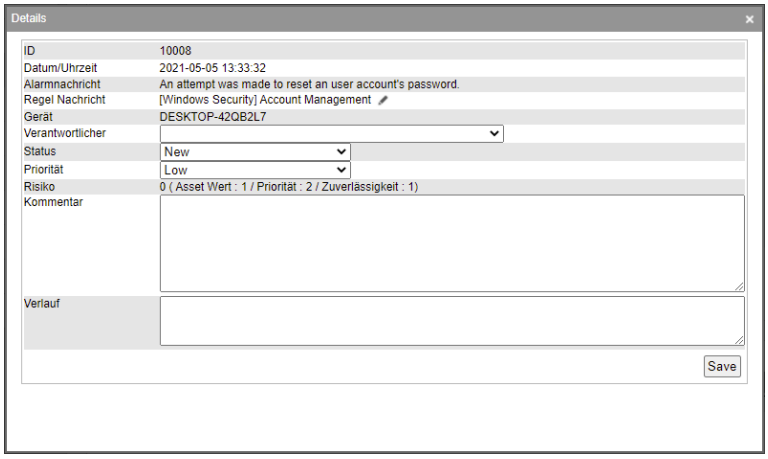

Abbildung 22: Alarmdetails

Entsprechend den Alarmierungseinstellungen unter „Alarmierung“ -> „Einstellungen“ werden Benutzer beim Auftreten von Alarmen per E-Mail benachrichtigt.

Abbildung 23: Alarmierungseinstellungen

Die Alarmierungsregeln, die vom Alert Parser abgearbeitet werden, können unter „Alarmierung“ -> „Regeln“ eingesehen und bearbeitet werden.

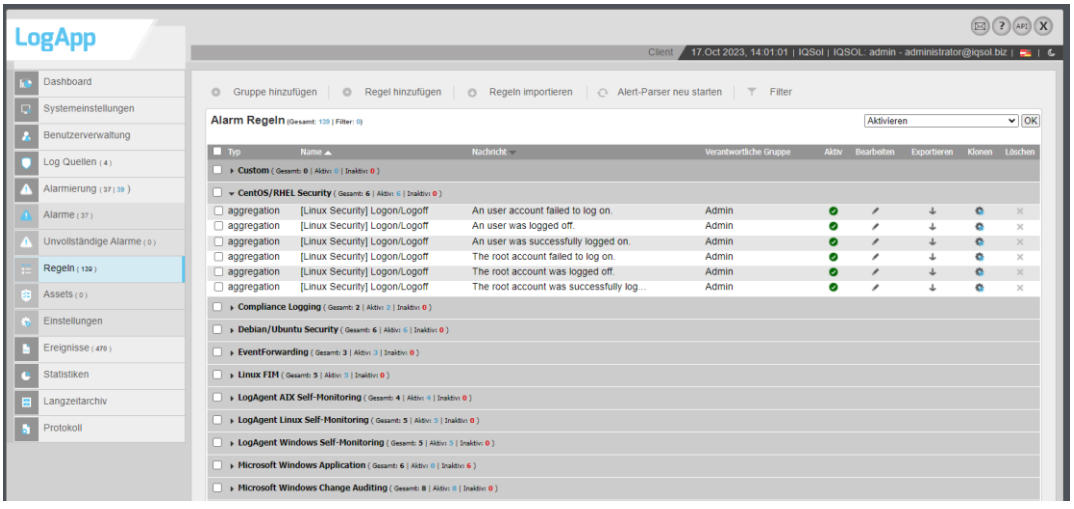

Abbildung 24: Alarmierungsregeln

Weitere Informationen über Alarme erhalten Sie in Kapitel 7. Alarme und Events

4 Allgemeine Einstellungen

4.1 Benutzerverwaltung

Die LogApp-Benutzerverwaltung ist sowohl in der zentralen Konfiguration als auch pro Mandant über den Menüpunkt „Benutzerverwaltung“ zugänglich. Die Berechtigungs-Struktur ist in Benutzer, Gruppen und Rollen unterteilt.

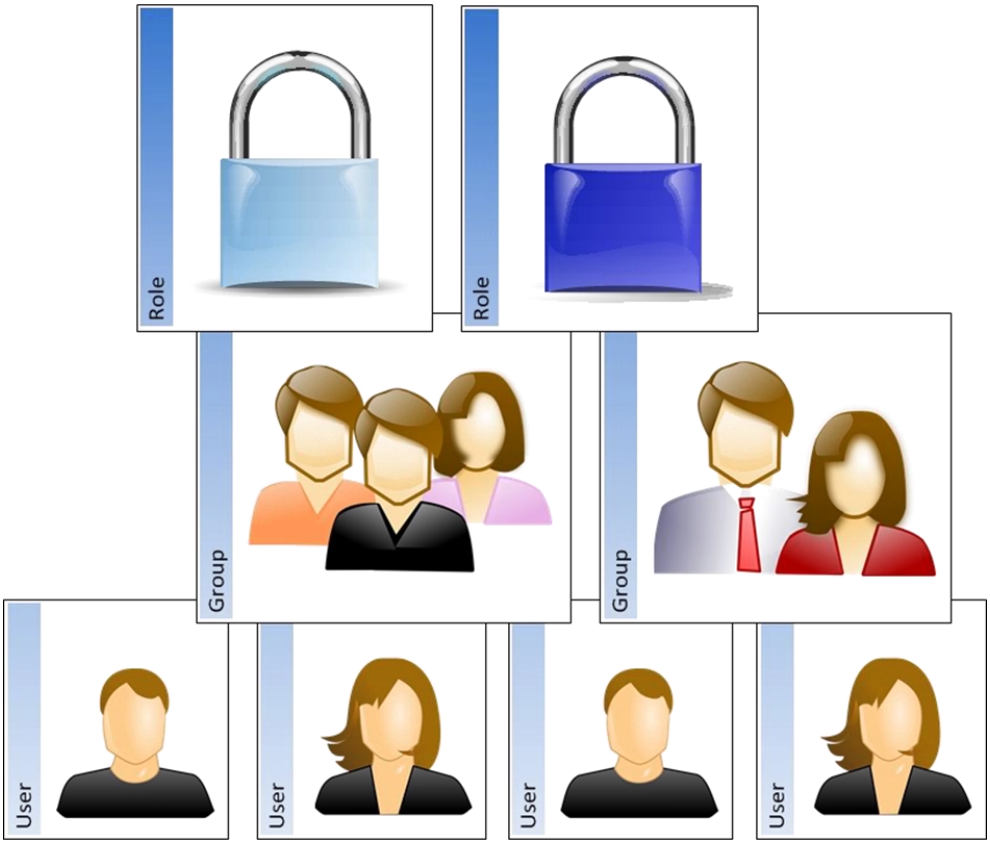

Abbildung 25: Berechtigungsstruktur

Ein Benutzer-Objekt definiert einen Benutzer-Account, der sich an der LogApp anmelden darf. Ein Benutzer kann Mitglied von mehreren Gruppen sein. Gruppen wiederum können eine oder mehrere Rollen zugeordnet haben. Eine Rolle ist mit speziellen Rechten (z.B. LogAgent Installation) verbunden.

4.1.1 Benutzer

Über dem Menüpunkt „Benutzer“ können bestehende Benutzer eingesehen bzw. bearbeitet und neue Benutzer angelegt werden.

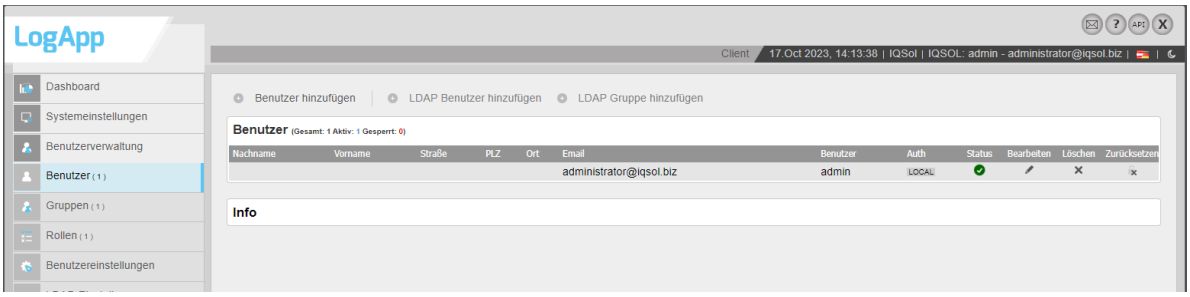

Abbildung 26: Benutzerverwaltung

Bestehende Benutzer können mit den Buttons in der Listenansicht bearbeitet werden. Benutzer können aktiviert bzw. deaktiviert werden (Button Status), Benutzerdetails können bearbeitet werden, Benutzer können gelöscht werden, und mit dem „Zurücksetzen“-Button kann das Passwort des eigenen Benutzers geändert bzw. die Passwörter anderer Benutzer zurückgesetzt werden.

Wird ein Passwort geändert, so gelten die in den Benutzereinstellungen definierten Kriterien. Zusätzlich dürfen auch hier folgende Zeichen nicht verwendet werden: ä, Ä, ö, Ö, ü, Ü, § ,€, ß.

Passwörter von anderen Benutzern dürfen nur von admins/superadmins zurückgesetzt werden.

Der „admin“/“superadmin“-Benutzer kann nicht deaktiviert oder gelöscht werden.

Neue lokale Benutzer können über den Button „Benutzer hinzufügen“ angelegt werden. Dabei müssen Vorname, Nachname, E-Mail-Adresse und Benutzername angegeben werden, optional kann eine Adresse hinterlegt werden. Mit der Checkbox „Monitor-Benutzer“ kann das automatische Session Timeout, das inaktive Benutzer abmeldet, deaktiviert werden. Monitor-Benutzer können verwendet werden, um die LogApp Oberfläche über einen längeren Zeitraum auf einem Monitor oder TV-Gerät anzuzeigen.

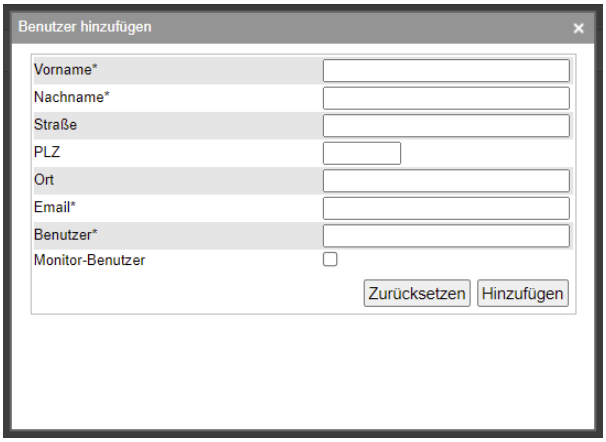

Abbildung 27: Benutzer hinzufügen

Mit dem Button „LDAP Benutzer hinzufügen“ können Benutzer von den hinterlegten LDAP Servern importiert werden (siehe 5.2.6 LDAP Einstellungen). Über das Textfeld „LDAP-Benutzer suchen (Regex)“ kann anhand einer Regex nach Benutzern gesucht werden.

Wählen Sie im LDAP Baum Benutzer aus, die sich an der LogApp anmelden können sollen.

Abbildung 28: LDAP Benutzer hinzufügen

Über „LDAP Gruppe hinzufügen“ ist es außerdem möglich eine LDAP Gruppe hinzuzufügen. Benutzer welche dieser Gruppe am AD zugeordnet sind, können sich dann bei der LogApp auhtentifizieren.

Auch hier ist es möglich zu suchen.

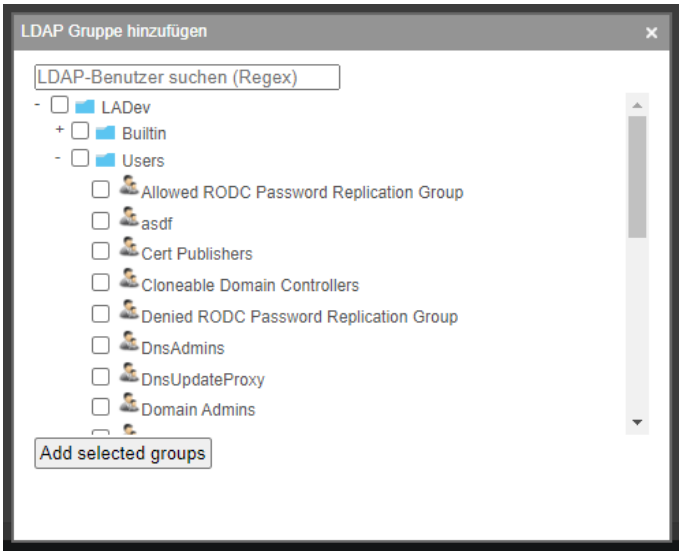

Abbildung 29: LDAP Gruppe hinzufügen

4.1.2 Gruppen

Alle LogApp Benutzer, sowohl in der Zentral- als auch in der Mandantenkonsole, müssen Mitglied einer Gruppe sein, um Rechte zu bekommen. In der Mandantenkonsole bilden Gruppenmitgliedschaften außerdem die Grundlage für die Alarmierung.

In der Gruppenverwaltung können mit dem Button „Gruppe hinzufügen“ neue Gruppen angelegt werden. Bestehende Gruppen können in der Listenansicht mit den entsprechenden Buttons bearbeitet werden.

Mit dem „Status“-Button können Gruppen deaktiviert bzw. wieder aktiviert werden. Deaktivierte Gruppen werden von der Alarmierung ausgenommen, die Benutzer in deaktivierten Gruppen können sich aber trotzdem an der LogApp anmelden. Der Gruppenname kann mit dem „Bearbeiten“-Button geändert werden.

Durch Klick auf „Hinzufügen“ können Benutzer zu Gruppen hinzugefügt werden. Mit dem „Entfernen“-Symbol direkt neben dem Benutzernamen werden Benutzer wieder aus Gruppen entfernt. Ganze Gruppen können mit dem „Löschen“-Button rechts in der Liste gelöscht werden. Die Gruppe „Admin“ kann nicht gelöscht werden.

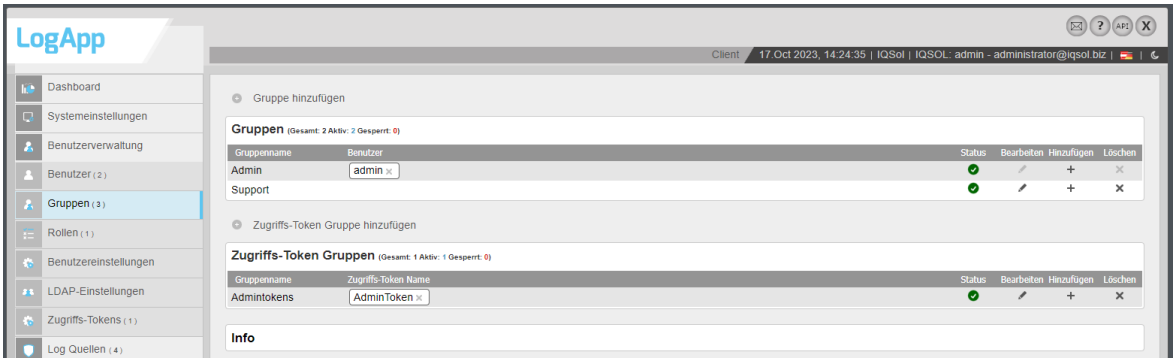

Abbildung 30: Gruppenverwaltung

Unterhalb der Benutzergruppen gibt es auch noch die Zugriffs-Token Gruppen, diese dienen dem Gruppieren von Zugriffstoken. Es sind die gleichen Aktionen möglich wie bei den Benutzergruppen, mit dem Unterschied, dass nur Zugriffstoken diesen Gruppen zugeordnet werden können.

Diese Gruppen können auch nicht zur Alarmierung verwendet werden.

4.1.3 Rollen

Mittels Rollen werden Berechtigungen in der LogApp Benutzeroberfläche abgebildet. Mit dem „Rolle hinzufügen“-Button können neue Rollen angelegt werden. Mit dem „Hinzufügen“-Button in der Listenansicht können Gruppen/Zugirffstoken Gruppen und Kontrollgruppen zu Rollen hinzugefügt werden. Mit dem „Entfernen“-Symbol direkt neben dem Gruppennamen können Gruppen wieder aus einer Rolle entfernt werden. Das „Löschen“-Symbol rechts in der Listenansicht löscht die ausgewählte Rolle.

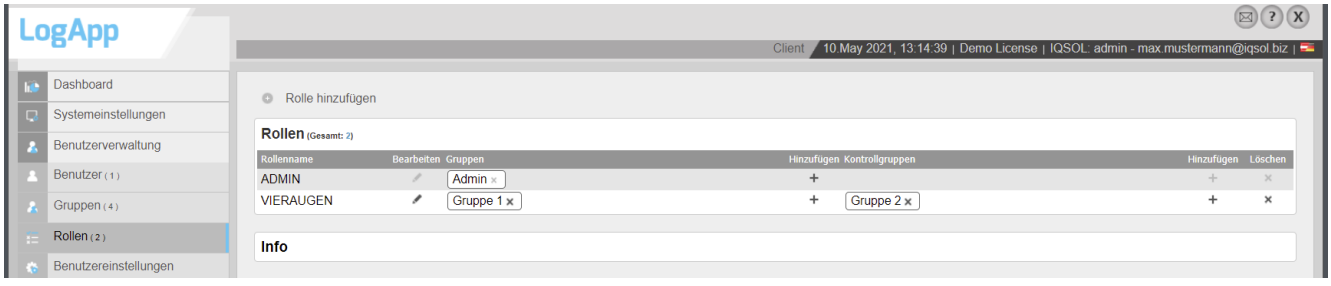

Abbildung 31: Rollenverwaltung

Mit dem „Bearbeiten“-Icon in der Listenansicht können Berechtigungen einer Rolle bearbeitet werden sowie das Vieraugenprinzip konfiguriert werden. Die einzelnen Berechtigungen sind nach den Menüpunkten, die für Gruppen in dieser Rolle zugänglich sind, strukturiert. Für die einzelnen Berechtigungen sind die Werte none (keine Berechtigung), readonly (nur lesender Zugriff) und full (schreib und leserechte) möglich.

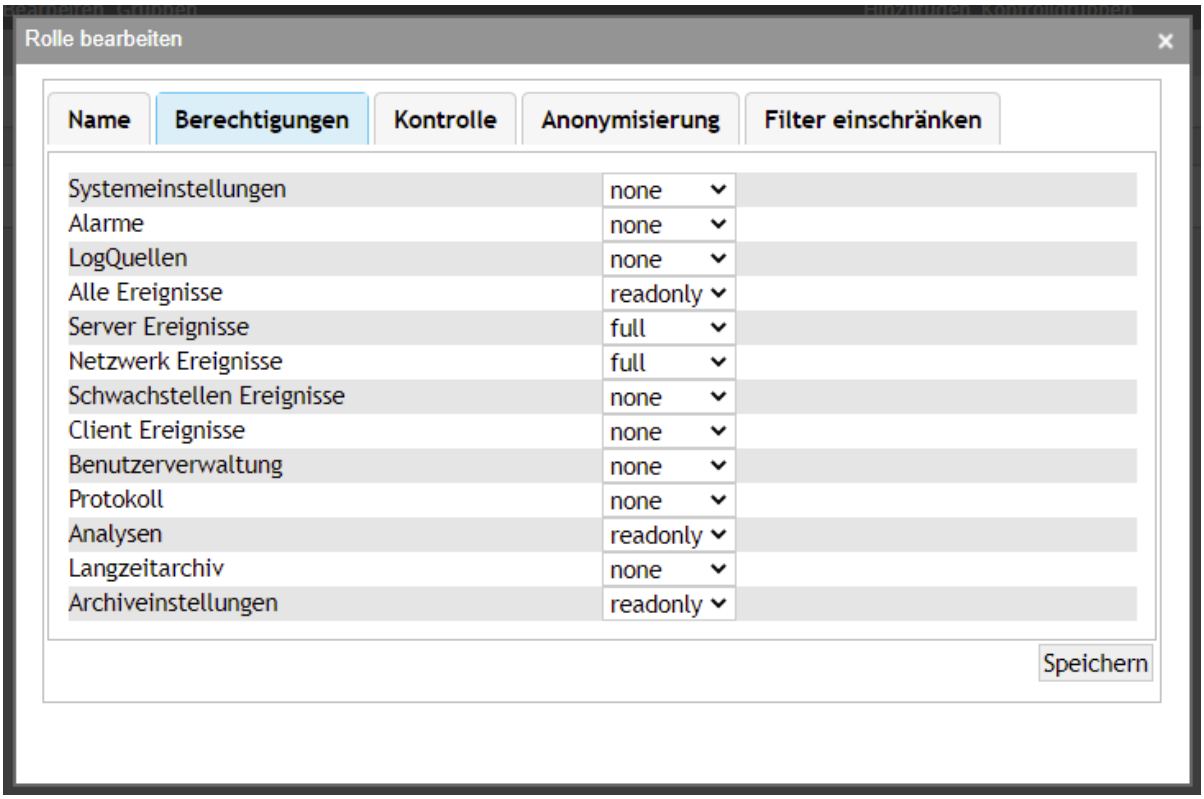

Abbildung 32: Berechtigungen einer Rolle

Vieraugenprinzip/Kontrolle

Bei aktiviertem Vieraugenprinzip ist eine zusätzliche Authentifizierung eines oder mehrerer Kontrollbenutzer zu dem Zeitpunkt, zu dem der Menüpunkt ausgewählt wird, erforderlich. Die Authentifizierung bleibt für die gesamte Benutzersession aufrecht.

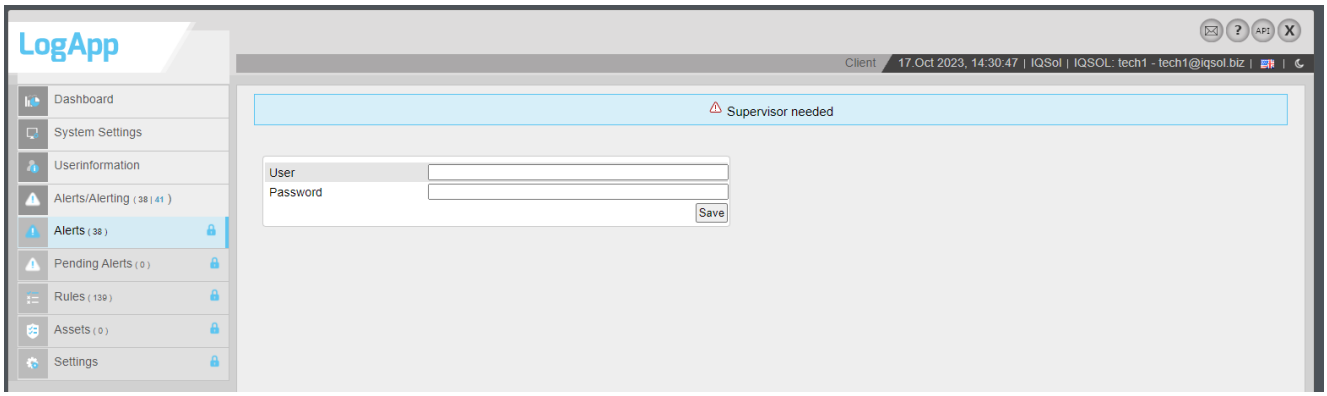

Abbildung 33 Vieraugenprinzip Authentifizierung

Zur Konfiguration eines Vieraugenprinzips, welches für jeden Menüpunkt einzeln definiert werden kann, sind am Tab „Kontrolle“ folgende Optionen verfügbar:

- Aktiviert: aktiviert das Vieraugenprinzip für die ausgewählten Menüelemente.
- Anzahl der Benutzer: die Anzahl der Benutzer aus den Kontrollgruppen, welche sich zusätzlich authentifizieren müssen, sobald der Menüpunkt gewählt wird.

- Verschiedene Gruppen: aktiviert die Option, dass die Kontrollbenutzer aus verschiedenen Kontrollgruppen kommen müssen.

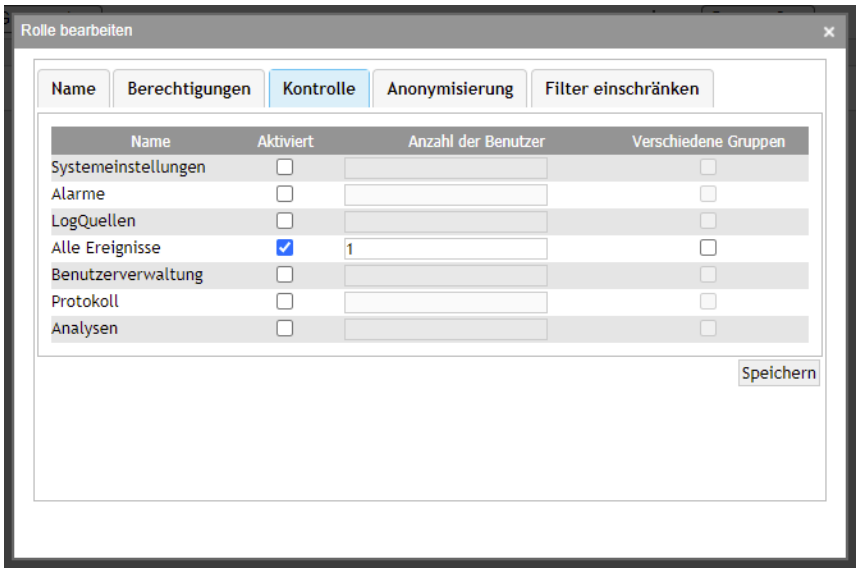

Abbildung 34 Vieraugenprinzip Einstellungen

Anonymisierung

Über den Tab Anonymisierung lassen sich bestimmte Werte in der Ereignisansicht verbergen.

Um dies zu bewerkstelligen muss zunächst ein Feld hinzugefügt werden, welches anonymisiert werden soll. Diesem Feld kann anschließend ein Name zugewiesen werden. Felder lassen sich über den Löschen-Button (rechts in der Titelzeile) jederzeit wieder löschen.

Zur Anonymisierung werden drei verschiedene Modi angeboten.

- Alles verstecken: Das ganze Feld wird versteckt, unabhängig vom Inhalt
- Alles verstecken mit RegEx: Auf der Basis eines Regulären Ausdrucks werden Felder, deren Werte eine positive Übereinstimmung liefern, versteckt.
- RegEx match verstecken: Dieser Modus ähnelt dem zweiten Modus. Im Unterschied zu diesem wird jedoch nicht das gesamte Feld versteckt, sondern nur jener Teil des Wertes welcher die Übereinstimmung lieferte maskiert.

Anschließend muss noch eine Konfigurationsgruppe ausgewählt werden. Die ausgewählte Anonymisierung wird nur auf diese angewendet. Hier können Alle, eine oder mehrere Konfigurationsgruppen zugewiesen werden.

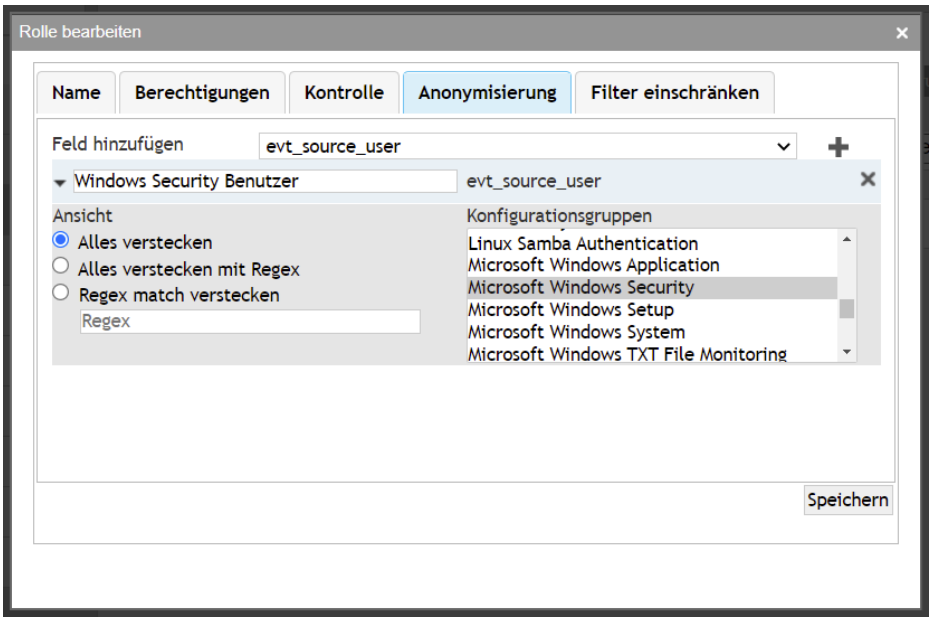

Abbildung 35: Anonymisierung

Beispiel:

Als Beispiel wird ein Logfileevent mit unten stehender evt_msg_short verwendet. Anschließend werden alle drei Modi zur Anonymisierung angewandt.

Evt_msg_short: `Administrator admin login failed from ssh(192.168.50.13) because of invalid password`

Modus/Ansicht	Angezeigte evt_msg_short
Alles Verstecken	Hier wird nichts in der Spalte (bei den Eventviews) oder dem Feld (bei Eventdetail) angezeigt.
Alles verstecken auf Basis von Regex Regex: **`admin login`**	Hier wird nichts in der Spalte (bei den Eventviews) oder dem Feld (bei Eventdetail) angezeigt.
Alles verstecken auf Basis von Regex Regex: **`admin logout`**	`Administrator admin login failed from ssh(192.168.50.13) because of invalid password`.
Regex match verstecken Regex: **`admin login`**	`Administrator ********** failed from ssh(192.168.50.13) because of invalid password`
Regex match verstecken Regex: **`admin logout`**	`Administrator admin login failed from ssh(192.168.50.13) because of invalid password`

Filter einschränken

Unter „Filter einschränken“ können gewisse Filter/Werte vom Gebrauch in der Eventansicht blockiert werden.

Hierzu muss wie bei der Anonymisierung ein Ereignisfeld hinzugefügt werden.

Ist dies geschehen kann unterschieden werden, ob der Filter generell blockiert wird (Alles Blockieren) oder nur gewisse Werte blockiert werden. Sollen nur gewisse Werte blockiert werden, so ist ein Regulärer Ausdruck zu verwenden. Bei einer erfolgreichen Übereinstimmung wird der betreffende Filter blockiert.

Wird ein Wert blockier so wird dies mit einer entsprechenden Meldung ausgegeben.

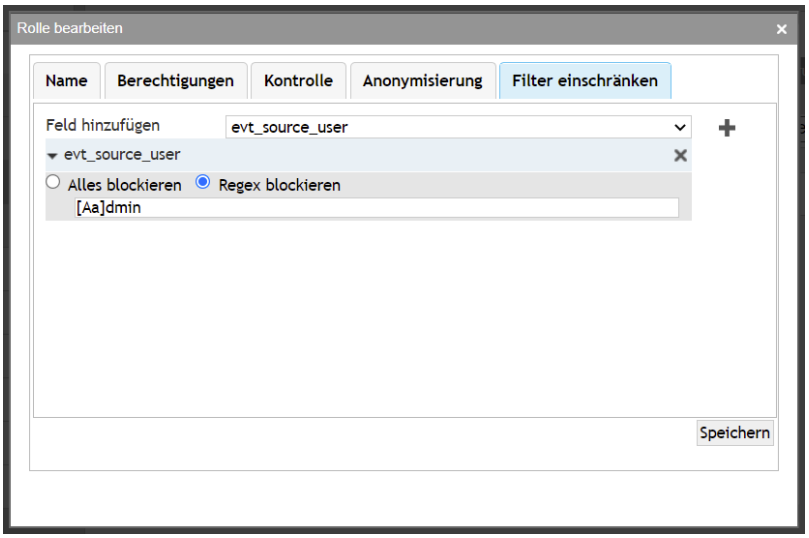

Abbildung 36: Filter einschränken

4.1.4 Benutzereinstellungen

Automatische Abmeldung bei Inaktivität

Diese Zeitspanne gibt an, wie lange ein Benutzer inaktiv auf der Weboberfläche sein darf, bevor er abgemeldet wird.

Sperren von inaktiven Benutzern

Bei Aktivierung dieser Option muss eine Zeitspanne in Tagen angegeben werden. Ist ein Benutzer in dieser Zeitspanne nicht aktiv, so wird dieser gesperrt. Ausgenommen sind nur Admin/Superadmin Benutzer.

Fehlgeschlagene Authentifizierung

Hier kann spezifiziert ab wie vielen fehlgeschlagenen Anmeldungsversuchen, innerhalb einer gewissen Zeitspanne (in Minuten), ein Benutzer für den Rest der Zeitspanne gesperrt wird.

Passwortrichtlinien

Unter den Passwortrichtlinien können eigene Richtlinien erstellt werden. Hierzu bieten sich folgende Möglichkeiten:

Passwort kann ablaufen:

Ist diese Option aktiviert, so kann ausgewählt werden, wie viele Tage ein Passwort gültig ist. Nutzer werden rechtzeitig vor Ablauf des Passwortes darüber informiert. Läuft ein Passwort ab so muss es direkt nach dem Login geändert werden.

Passwortkomplexität: es besteht die Möglichkeit bei Passwörtern eine Mindestlänge festzulegen. Außerdem lässt sich mit der Länge der Passwort History festlegen, wie viele vorhergegangene Passwörter nicht verwendet

werden dürfen. Es kann außerdem noch aktiviert werden ob das Passwort den Benutzernamen enthalten darf. Abschließend kann festgelegt werden, ob das Passwort Sonderzeichen enthalten muss.

Zwei-Faktor-Authentifizierung (2FA)

Hier kann angegeben werden ob/welche Zwei-Faktor-Authentifizierung für den Login verwendet werden soll.

Wird eine Methode zur 2FA ausgewählt so können sich nur mehr User mit gültiger Konfiguration anmelden. Die einzigen ausgenommen User sind die jeweiligen Admin/Superadmin User.

None

Es wird keine 2FA verwendet.

FIDO2

Vorraussetzung um FIDO2 als zweiten Faktor einsetzen zu können ist es, ein FIDO2 fähiges Gerät zu haben und ein gültiges Zertifikat auf der LogApp eingespielt zu haben.

Konfiguration:

Um FIDO2 zu verwenden, muss zuerst in den Benutzereinstellungen die FIDO2 Domäne hinterlegt sein. Diese Domäne muss gleich dem dnsnamen sein, der zum Aufruf der LogApp verwendet wird.

Anschließend können einzelnen Benutzer mehrere Geräte hinzugefügt werden.

Hierzu kann bei einem Benutzer ein Anzeigename eingetragen werden, und mit regisitrieren registriert werden.

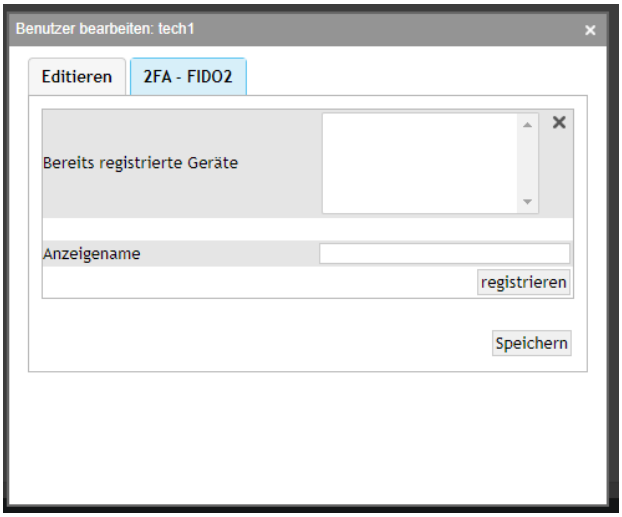

Abbildung 37 Registrierung FIDO2

Hier können ebenfalls bereits registrierte Geräte entfernt werden.

YubiKey OTP:

Yubico OTP wird für die 2FA verwendet. Yubico OTP kann mit jedem YubiKey und jedem Browser verwendet werden.

Konfiguration:

Um einen YubiKey einem User zuzuordnen gibt es mehrere Möglichkeiten, entweder man trägt die Felder Public Identity, private Identity und geheimer Schlüssel von einer bestehenden Konfiguration ein oder man generiert sich neue Schlüssel, welche danach auf dem YubiKey konfiguriert werden können. **!!! ACHTUNG!!!** Sollten neue Schlüssel generiert werden so wird der verwendete Slot überschrieben und kann nicht mehr mit anderen zuvor gespeicherten Applikationen verwendet werden.

Anschließend muss im Feld OTP noch ein OneTimePassword vom vollständig konfigurierten YubiKey eingegeben werden. Danach kann die Konfiguration mit speichern abgeschlossen werden.

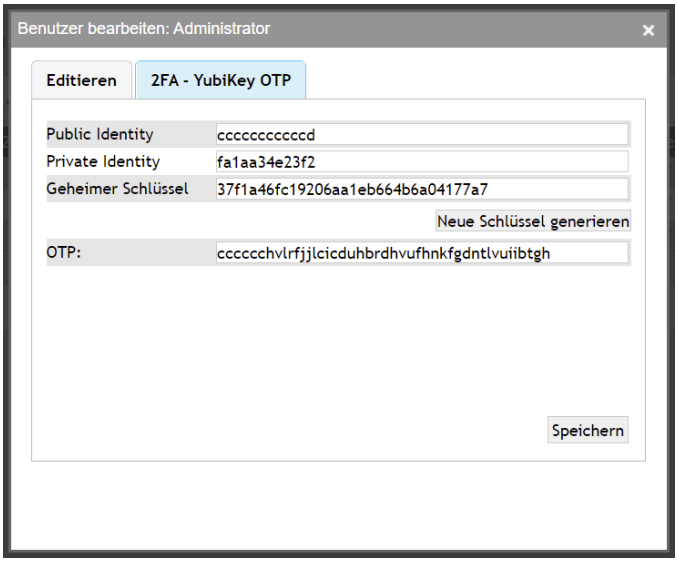

Abbildung 38 Registrierung YubiKey OTP

AMS SMS:

AMS SMS verwendet einen zu konfigurierenden AMS und versendet über diesen eine SMS an den Benutzer.

Konfiguration:

Um AMS SMS zu verwenden müssen in den Benutzereinstellungen neben der Zwei-Faktor-Authentifizierung „AMS SMS“ auch die Anmeldeeinstellungen des AMS hinterlegt werden. Wo diese zu finden sind entnehmen sie bitte dem Benutzerhandbuch des AMS.

Um einen Benutzer zu aktivieren, muss im Dialog Benutzer bearbeiten der Tab 2FA- AMS SMS ausgewählt werden und eine Telefonnummer hinterlegt werden. In diesem Fenster lässt sich auch ein Code zur Überprüfung senden und validieren.

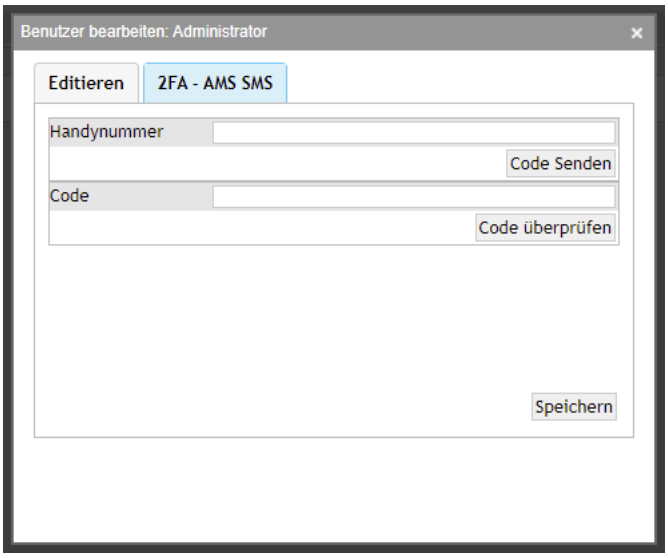

Abbildung 39 Registrierung für AMS SMS

Radius:

Eine weitere Möglichkeit für 2FA stellt ein Radius dar. Um einen Radius zu verwenden wird die Ip Adresse des Radius Servers und das der LogApp zugewiesene Geheimnis benötigt.

Die vorher durchzuführende Konfiguration auf dem Radius entnehmen sie bitte dessen Dokumentation.

Konfiguration:

Nachdem IP Adresse und Geheimnis des Radius bei den Benutzereinstellungen vorgenommen wurden, muss der zu aktivierende User editiert werden.

Im Tab „2FA FortiAuthenticator“ muss nun der Radius Benutzername eingegeben werden, sollte dieser vom Benutzernamen auf der LogApp abweichen.

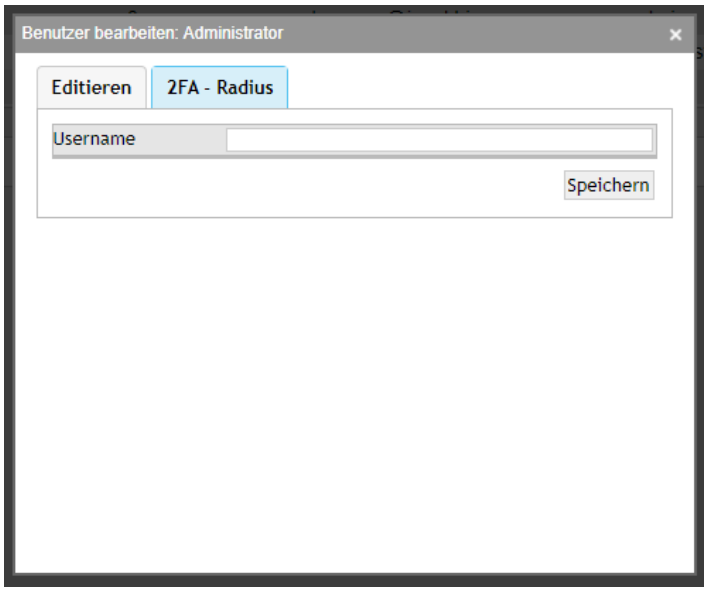

Abbildung 40 Registrierung für Radius

MS Authenticator/Google Authenticator – TOTP (Time-based One-time Password):

Die Authentifizierung erfolgt mit einem "Time-based One-time Password(TOTP)" über Microsoft Authenticator oder Google Authenticator. Andere TOTP-Authenticator-Apps können ebenfalls verwendet werden. Diese Apps generieren einmalige Token auf Ihrem Gerät, die in Kombination mit Ihrem Passwort verwendet werden.

Konfiguration:

Wählen Sie unter Benutzerverwaltung->Benutzereinstellungen->Zwei-Faktor-Authentifizierung die Option „MS Authenticator/Google Authenticator – TOTP“ und klicken Sie auf Speichern. Danach gehen Sie zu Benutzerverwaltung->Benutzer und klicken auf "Benutzer bearbeiten" für den Benutzer, den Sie konfigurieren möchten. Im Tab „2FA – TOTP“ wird ein QR-Code angezeigt. Scannen Sie nun diesen QR-Code mit Ihrer Authenticator-App. Nun sollte die Zwei-Faktor-Authentifizierung über TOTP korrekt konfiguriert sein.

Wenn Sie sich nun mit einem Benutzer anmelden, müssen Sie das Einmalkennwort aus der Authenticator-App im Anmeldefenster eingeben.

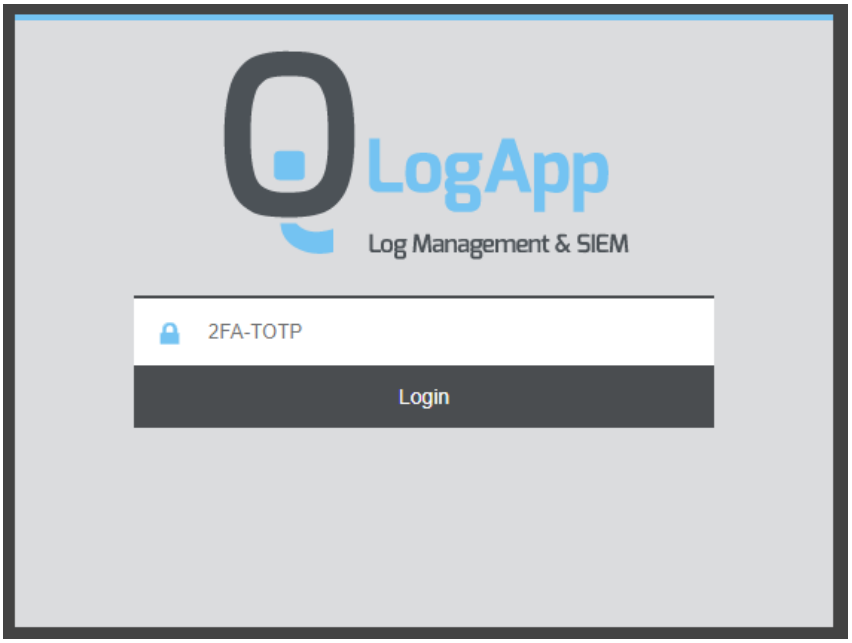

Abbildung 41: Einmalkennwort Eingabe bei Login für TOTP

!!! ACHTUNG !!! Damit die TOTP-Authentifizierung richtig funktioniert, muss die Zeit der LogApp auf die Sekunde genau eingestellt sein!

4.1.5 LDAP Einstellungen

In den LDAP Einstellungen können mehrere LDAP Server für die Benutzerauthentifizierung hinterlegt werden. Zur Abfrage und Authentifizierung werden die Server der Reihe nach herangezogen. Sollte ein Server nicht erreichbar sein, bzw. die Authentifizierung fehlschlagen, so wird der nächste Server für diesen Vorgang verwendet. Sollte der Vorgang bei allen angegebenen Servern fehlschlagen, so wird dies als Fehler gehandhabt und entsprechend protokolliert.

Geben Sie Servername oder IP von bis zu 3 Servern, Port, Authentifizierungsdaten und Domain/Organisation an. Beim Speichern wird die Verbindung zum LDAP Server getestet und eine Statusmeldung ausgegeben.

Bei Domain/Organisation lassen sich verschiedenste Optionen angeben. Hierbei kann die ganze Hierarchie zur Suche herangezogen werden (z.B. dc=example, dc=com), auf Container beschränkt werden (z.B. CN=vienna, dc=example, dc=com) oder auch auf Organisationseinheiten zurückgegriffen werden (z.B. ou=Developers,

dc=example, dc=com) Domäne/Organisation unterstützt auch Zeichenketten welche vom FortiAuthenticator verwendet werden (z.B. uid=developers, dc=example, dc=com).

Sollte LDAPS verwendet werden, so wird das momentan verwendete Zertifikat angezeigt. Durch den Button „Zertifikat austauschen“ kann dieses ausgewechselt werden.

Das Für LDAPS verwendete Zertifikat muss ein Rootzertifikat oder ein Zertifikat zur Authentifizierung sein, welches im Base64 Format exportiert wurde.

Als Verzeichnisdienst stehen Active Directory und FortiAuthenticator zu Verfügung. Bei gewähltem Active Directory kann jedoch jedes beliebige LDAP verwendet werden. Hierbei muss ein gültiger Bind User spezifiziert sein (z.B. cn=LDAP-Bind-User,ou=service,ou=ad-users,dc=example,dc=com).

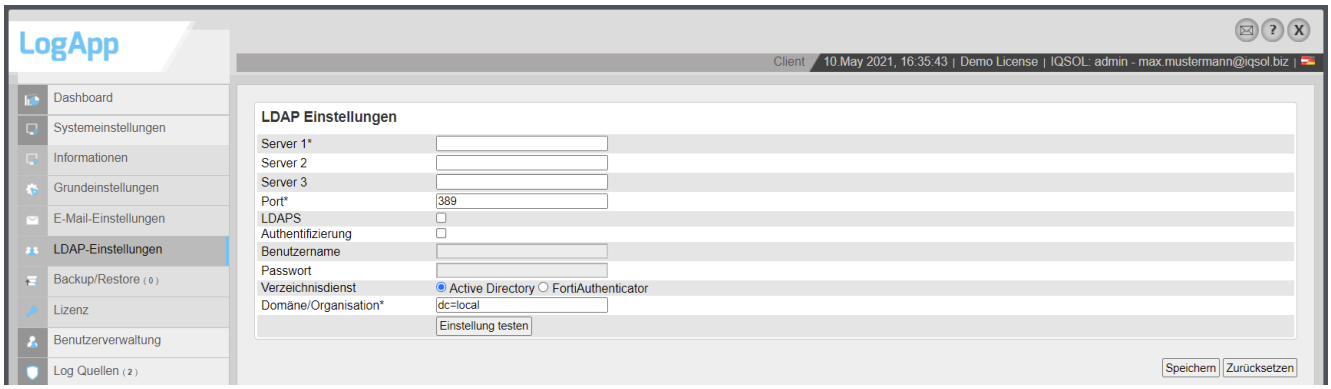

Abbildung 42: LDAP Einstellungen

Mit dem Button „Einstellungen testen“, kann überprüft werden, ob die Authentifizierung, bzw. die Abfrage von Daten funktioniert. Hierbei liefert die LogApp Ergebnisse für jeden angegebenen Server.

LDAP Benutzer können in der Benutzerverwaltung (siehe 5.5 Benutzerverwaltung) importiert werden.

Die LDAP Einstellungen gelten nur für die Zentralkonsole und können für jeden Mandanten unabhängig getroffen werden.

4.1.6 Zugriffs-Tokens

Im Menüpunkt Zugriffs-Tokens können Tokens für die REST API angelegt werden. Klickt man auf den Button „JWT Token generieren“ kann man einen Namen vergeben und es wird einem der Token angezeigt. Diesen muss man extern zwischenspeichern, weil dieser nicht mehr angezeigt wird.

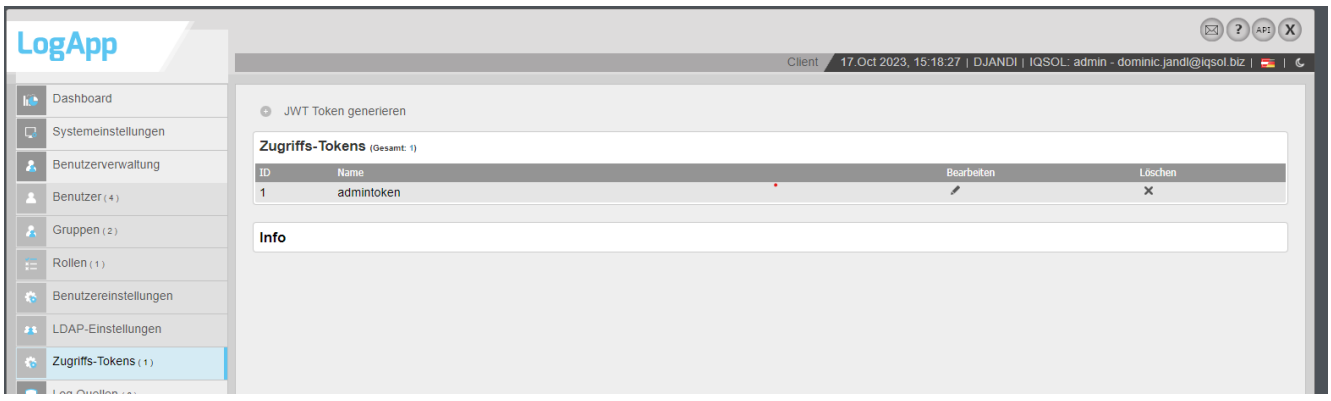

Abbildung 43: Zugriffs-Token Verwaltung

Tokens können außerdem noch editiert, d.h. der Name geändert, und gelöscht werden.

Die Berechtigungen der Tokens werden ähnlich wie bei Benutzern über eigene Token-Gruppen, welche man einer Rolle zuweisen kann, vergeben.

4.2 E-Mail-Einstellungen

In den E-Mail-Einstellungen der Zentralkonsole sollte ein SMTP Server für Benachrichtigungen an den Superadmin konfiguriert werden. Benachrichtigt werden kritische Systemereignisse wie z.B. ein hoher Belegungsgrad der Festplatte. Die Einstellungen können mit dem Button „Testmail senden“ getestet werden, der (Super)Admin bekommt ein Mail an die hinterlegte E-Mail-Adresse.

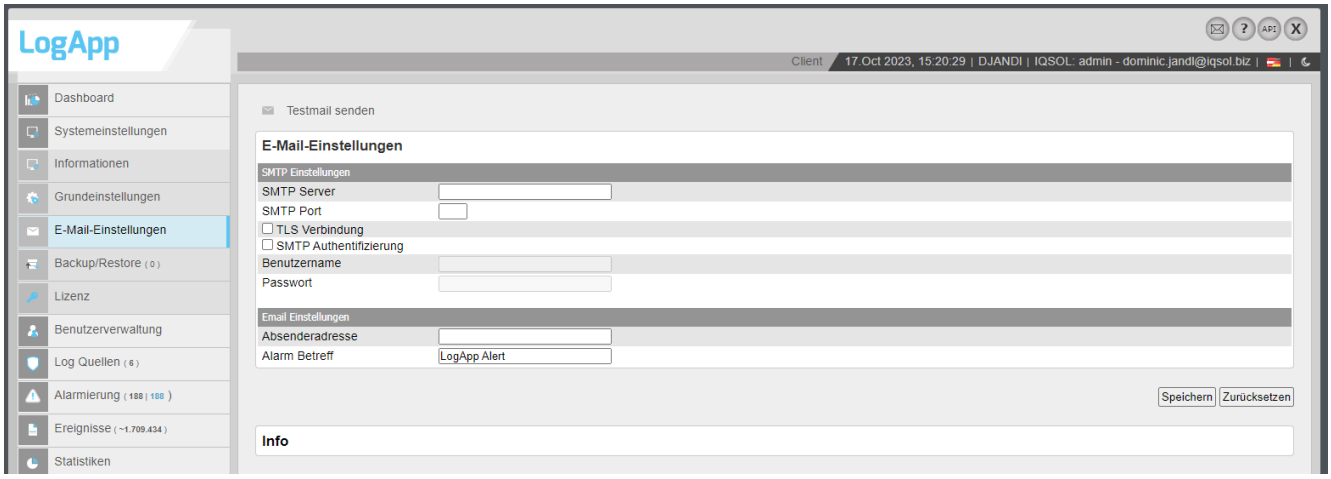

Abbildung 44: E-Mail-Einstellungen

Die E-Mail-Einstellungen gelten nur für die Zentralkonsole und müssen für jeden Mandanten unabhängig getroffen werden.

5 Zentrale Konfiguration

In der zentralen Konfiguration (Superadmin) werden Einstellungen vorgenommen, welche alle Mandanten gleichermaßen betreffen.

5.1 Dashboard

Das Dashboard der zentralen Konfiguration zeigt einen schnellen Überblick über den Status des Systems.

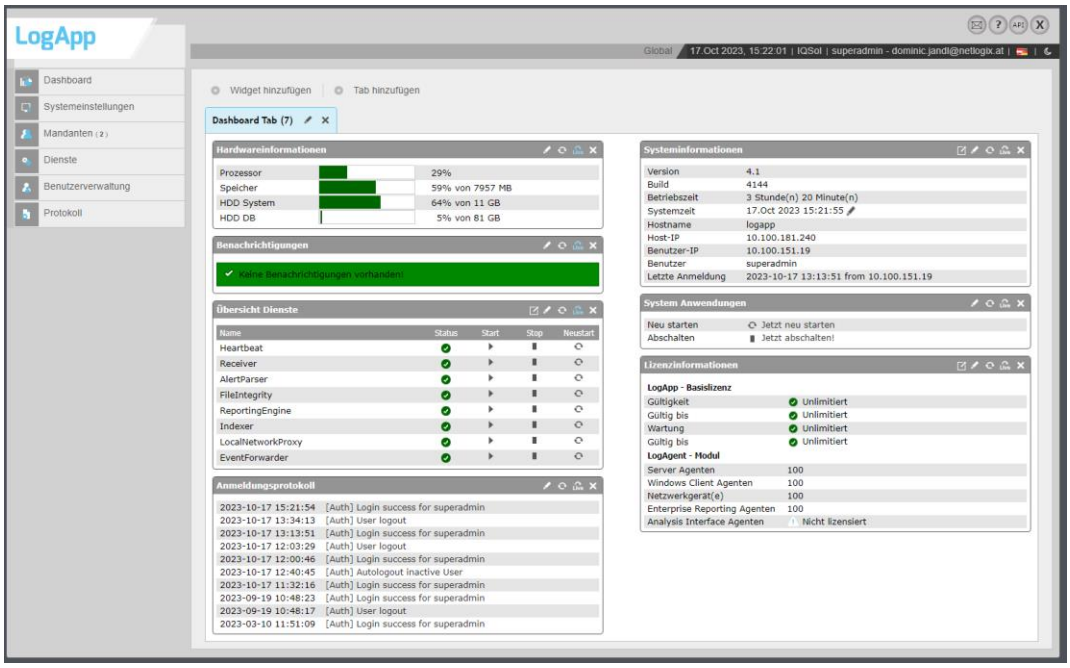

Abbildung 45: Dashboard zentrale Konfiguration

Der folgenden Tabelle können sie mögliche Widgets am Superadmin Dashboard entnehmen.

Widget	Beschreibung
Hardwareinformation	Zeigt die Auslastung des Prozessors, des Hauptspeichers sowie der System- und Datenplatte. Bei Überschreitung der gesetzten Grenzwerte (siehe auch CLI Befehl dblimits) wird per E-Mail an den Administrator eine Warnung versandt **(die Konfiguration eines gültigen E-Mail-Servers sowie einer gültigen E-Mail-Adresse für den Administrator ist für diese Funktion unbedingt erforderlich!).** Wird der Mauszeiger auf den Balken neben den Prozessor geführt, so erscheint eine Information über die Prozessorkerne und die Taktung.
Systeminformation	Allgemeine Informationen zum aktuellen System. Neben der Systemzeit befindet sich ein „Bearbeiten“ – Icon. Wird dieses geklickt, so gelangt man in den Bereich „Systemeinstellungen“ -> Informationen. Dort ist es möglich, die aktuelle Systemzeit zu ändern. (Siehe Kapitel 5.2.1) Dieses Widget besitzt einen Querlink. Im Header ist das „Springe zu -Icon“ zu finden. Wird dies geklickt, so gelangt man zum Menüpunkt „Systemeinstellungen“ -> „Informationen“
Benachrichtigungen	Hinweise zum Status des Systems wie z.B. der fehlenden Konfiguration eines E-Mail-Servers oder gestoppten Diensten. Bei gestoppten Diensten wird zusätzlich per E-Mail an den Administrator eine Warnung versandt **(die Konfiguration eines gültigen E-Mail-Servers sowie einer gültigen E-Mail-Adresse für den Administrator ist für diese Funktion unbedingt erforderlich!).**

Lizenzinformation	Informationen über die aktuell aktive Lizenz und die Aufteilung der Lizenzen. Dieses Widget besitzt einen Querlink. Im Header ist das „Springe zu“-Icon zu finden. Wird dies geklickt, so gelangt man zum Menüpunkt „Systemeinstellungen“ -> „Lizenz“
Übersicht Dienste	Übersicht über alle Dienste, deren Status und die Möglichkeit, diese zu stoppen und zu starten.
System Anwendungen	Neustarten und Herunterfahren des Systems.
Anmeldungsprotokoll	Dieses Widget zeigt die Anmeldeversuche des jeweiligen Bereichs an.

Tabelle 3: Widgets Dashboard Zentralkonsole

Die Widgets des Dashboards können auf verschiedene Tabs verteilt werden. Standardmäßig befinden sich alle im „Dashboard Tab“. Um einen neuen Tab hinzuzufügen klicken Sie auf den Button „Tab hinzufügen“. Dort kann ein Name vergeben und Widgets diesem Tab zugeordnet werden.

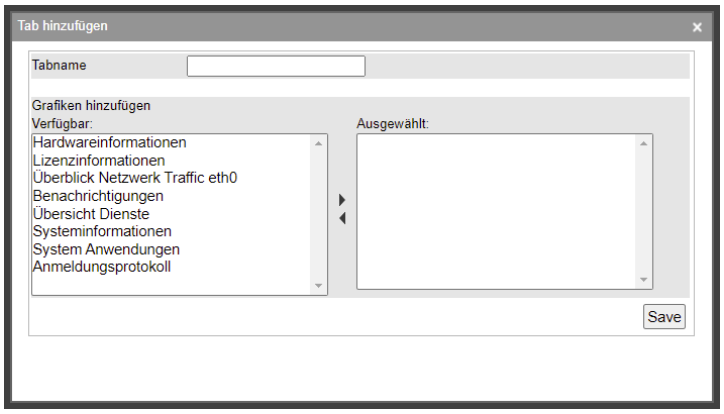

Abbildung 46: Tab hinzufügen

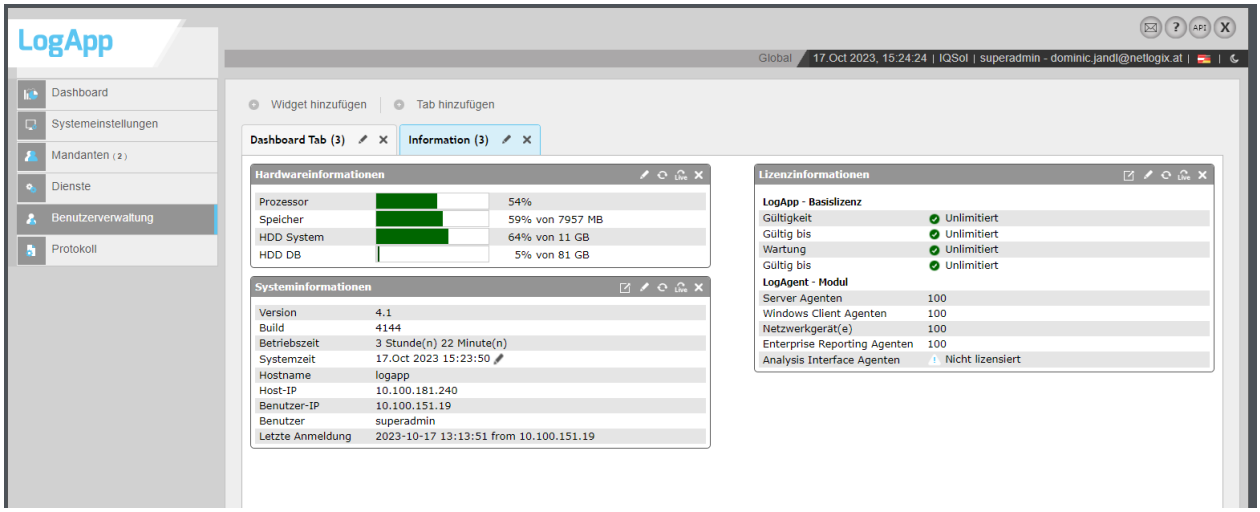

Abbildung 47: Mehrere Tabs

Neben dem Tab-Namen werden die Anzahl der darin enthaltenen Widgets angezeigt. Daneben befinden sich ein „Tab bearbeiten“ - Icon womit der Name des Tabs geändert werden kann.

Wird der Tab nicht mehr benötigt, so kann dieser durch das „Tab löschen“ - Icon gelöscht werden. Sind in diesem Tab noch Widgets enthalten, so können sie entweder „versteckt“ oder in einen anderen Tab verschoben werden. Der Standard - Tab, benannt „Dashboard Tab“, kann nicht gelöscht werden, es ist jedoch möglich, den Namen zu ändern.

Bei jedem Widget besteht die Möglichkeit, verschiedene Aktionen auszuführen. Folgende Aktionen sind verfügbar:

Widget - Aktionen	
Querlink	Springe zum dazugehörigen Menüpunkt.
Widget bearbeiten	Änderung des Namens und Zuordnung zu einem anderen Tab
Aktualisieren	Aktualisieren des Widgets (Fenstergrößenänderung, aktuelle Daten einsehen, . . .)
Liveupdate	Ist das Icon vollständig gefärbt, so ist das Liveupdateintervall aktiviert. In diesem Modus wird das Widget alle 5 Sekunden aktualisiert. Ist das Icon nur teilweise gefärbt, so ist das Liveupdateintervall deaktiviert.
Schließen	Das Widget wird „versteckt“. Es kann danach über den „Widget hinzufügen“ – Button wieder hinzugefügt werden. Widgets der Zentralen Konfiguration sind Standard - Widgets und können nicht gelöscht werden.

Tabelle 4: Widgets Dashboard Zentralkonsole

5.2 Systemeinstellungen

5.2.1 Informationen

In den Informationen sind System – und Hardwareinformationen ersichtlich.

Um die Systemzeit zu ändern, klicken Sie hierzu auf das Icon „Zeit bearbeiten“ neben der aktuellen Systemzeit.

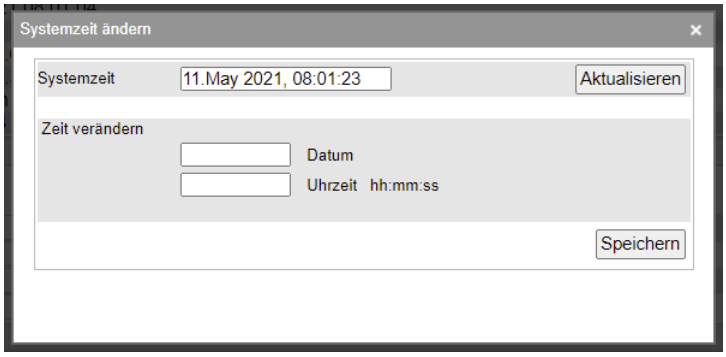

Abbildung 48: Systemzeit ändern

Neben „Systemzeit“ ist die aktuell gesetzte Zeit ersichtlich. Mit einem Klick auf „Aktualisieren“ wird die Zeit aktualisiert.

Bei der Eingabe werden Datum und Uhrzeit eingegeben und als neue Systemzeit festgelegt.

5.2.2 Netzwerk

Im Widget Netzwerkkarte können weitere Netzwerkkarten angelegt, geändert und gelöscht werden. Das Interface eth0 ist unveränderlich.

Unter „Systemeinstellungen“ kann die IP-Adresse des verwendeten DNS Servers bearbeitet werden. Stellen Sie sicher, dass die LogApp einen gültigen DNS Server verwendet, ansonsten kann es zu Komplikationen bei der Verwendung von Hostnamen kommen.

Unter „Hostname“ kann der Hostname geändert werden.

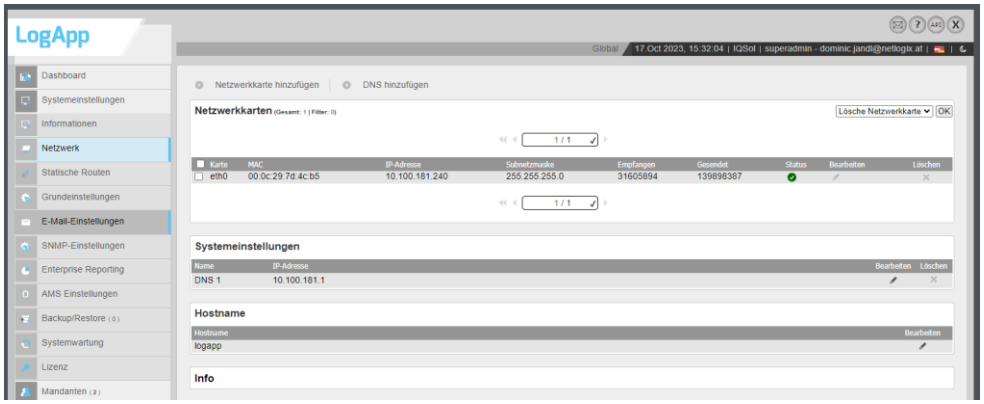

Abbildung 49: Netzwerk

5.2.3 Statische Routen

Für die Anbindung von LogAgents müssen gegebenenfalls statische Routen für fremde Subnetze hinterlegt werden.

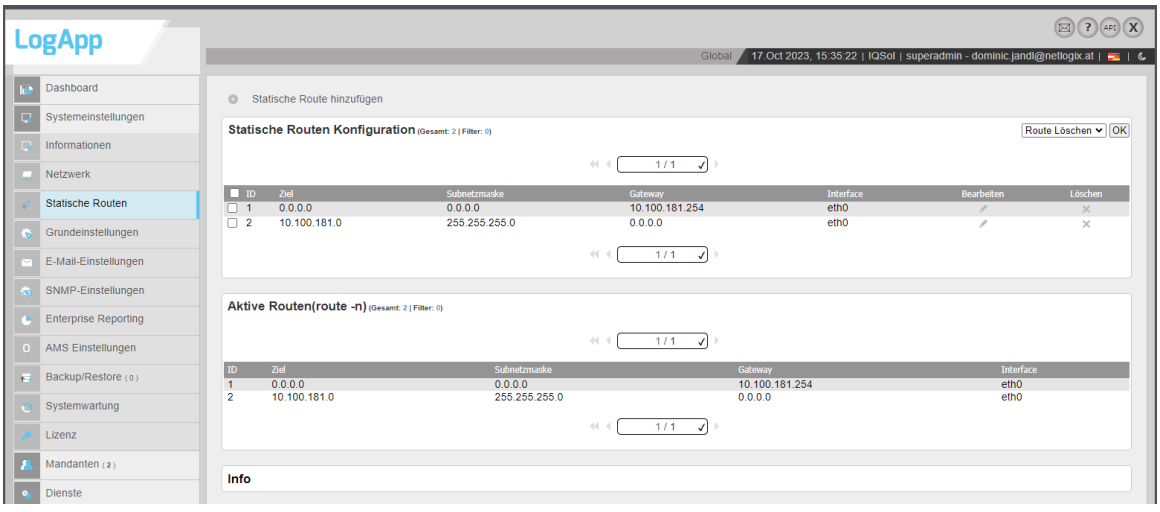

Abbildung 50: Statische Routen

Achtung: Werden benötigte Routen gelöscht, kann das die Funktionsweise der LogApp und die Kommunikation mit LogAgents negativ beeinflussen.

5.2.4 Grundeinstellungen

In den Grundeinstellungen der Zentralkonsole können folgende wichtige Optionen für das System festgelegt werden:

Option	Beschreibung
Allgemeine Einstellungen	
Aktualisierungsintervall	Intervall in Sekunden, in dem Listenansichten (Ereignisse/Alarme) bei aktiviertem Live Update neu geladen werden.
Einträge pro Seite	Anzahl der Einträge pro Seite in Listenansichten
Löscheinstellungen	
Protokoll	Anzahl der Tage, nach denen Protokolleinträge aus dem Archiv gelöscht werden.
VMware-Tools	
VMware-Tools installieren	Installiert VMware-Tools auf der LogApp, nur für virtuelle Maschinen unter VMware empfohlen
Hyper-V Integration Services	
Hyper-V Integration Services Installieren	Installiert Hyper-V Integration Services
HTTPS-Zertifikate	
CSR Herunterladen	Hier kann ein CSR generiert werden, mithilfe dessen sich ein Zertifikat für den Webserver erstellen lässt. Um mehrere SAN Werte angeben zu können, müssen diese mittels Beistriches getrennt werden. Domänen werden mittels „DNS=“ gekennzeichnet und IP-Adressen mittels „IP=“ (bei beide Präfixen darf kein Leerzeichen enthalten sein). Z.B.: „DNS=logapp, IP=10.100.181.30“; „DNS=logapp, DNS=logapp2“
Zertifikat (PEM oder PKCS12)	Upload für ein Zertifikat im PEM (Dateiendung .pem)- oder PKCS12- Format (Dateiendungen .cer,.crt,.pfx) für die HTTPS-Verbindung mit der Web GUI
Privater Schlüssel (PEM)	Privater Schlüssel des HTTPS-Zertifikats im PEM Format (Dateiendung. pem). Dieser ist nur notwending wenn ein Zertifkat im PEM Format verwendet wird, welches nicht aus dem CSR generiert wurde, welcher über die Web GUI heruntergeladen werden kann.
Passwort des privaten Schlüssels	Passwort des privaten Schlüssels, falls vorhanden
REST API - Zertifikate	

CSR Herunterladen	Hier kann ein CSR generiert werden, mithilfe dessen sich ein Zertifikat für den Webserver erstellen lässt. Um mehrere SAN Werte angeben zu können, müssen diese mittels Beistriches getrennt werden. Domänen werden mittels „DNS=“ gekennzeichnet und IP-Adressen mittels „IP=“ (bei beide Präfixen darf kein Leerzeichen enthalten sein). Z.B.: „DNS=logapp, IP=10.100.181.30“; „DNS=logapp, DNS=logapp2“
Zertifikat (PEM oder PKCS12)	Upload für ein Zertifikat im PEM (Dateiendung .pem)- oder PKCS12- Format (Dateiendungen .cer,.crt,.pfx) für die REST API-Verbindung
Privater Schlüssel (PEM)	Privater Schlüssel des REST API-Zertifikats im PEM Format (Dateiendung. pem). Dieser ist nur notwending wenn ein Zertifkat im PEM Format verwendet wird, welches nicht aus dem CSR generiert wurde, welcher über die Web GUI heruntergeladen werden kann.
Passwort des privaten Schlüssels	Passwort des privaten Schlüssels, falls vorhanden
NTP Server Einstellungen	
NTP Server	NTP Zeitserver, von dem die aktuelle Zeit bezogen werden kann (IP Adresse oder FQDN, falls DNS Server angebunden ist)
NTP Backup Server	NTP Backup Zeitserver, von dem die aktuelle Zeit bezogen werden kann, falls der NTP Server nicht zur Verfügung steht (IP Adresse oder FQDN, falls DNS Server angebunden ist)
Authentifizierungslog	
IP, Port	Empfänger der lokalen Authentifizierungslogs (CLI-Authentifizierungen). Die Logs können an die LogApp selbst (Default-Einstellung) oder an eine fremde LogApp gesendet werden.
EventForwarder	
Der EventForwarder dient dem Weiterleiten von Events an eine andere LogApp. Aktiviert man den EventForwarder so wird man aufgefordert das Default-Zertifikat der Ziel-LogApp anzugeben. Dieses muss vorher von jener heruntergeladen werden.	
IP	IP der Ziel-LogApp
Mandant	Mandant unter dem die Quell-LogApp aufscheinen soll
Heartbeat Port	Heartbeat Port der Ziel-LogApp
Event Port	Event Port der Ziel-LogApp
Gateway	
Default Gateway ETH1	Gateway für das ETH1 Interface, das beim Anlegen von Routen automatisch vorgeschlagen wird.

Tabelle 5: Grundeinstellungen in der Zentralkonsole

5.2.5 E-Mail-Einstellungen

Siehe Kapitel 4 - Allgemeine Einstellungen.

5.2.6 LDAP Einstellungen

Siehe Kapitel 4 - Allgemeine Einstellungen.

5.2.7 SNMP Einstellungen

SNMP kann im „Superadmin“ Bereich unter „SNMP Einstellungen“ aktiviert werden. Dabei kann zwischen der SNMP Version 2 und 3 ausgewählt werden.

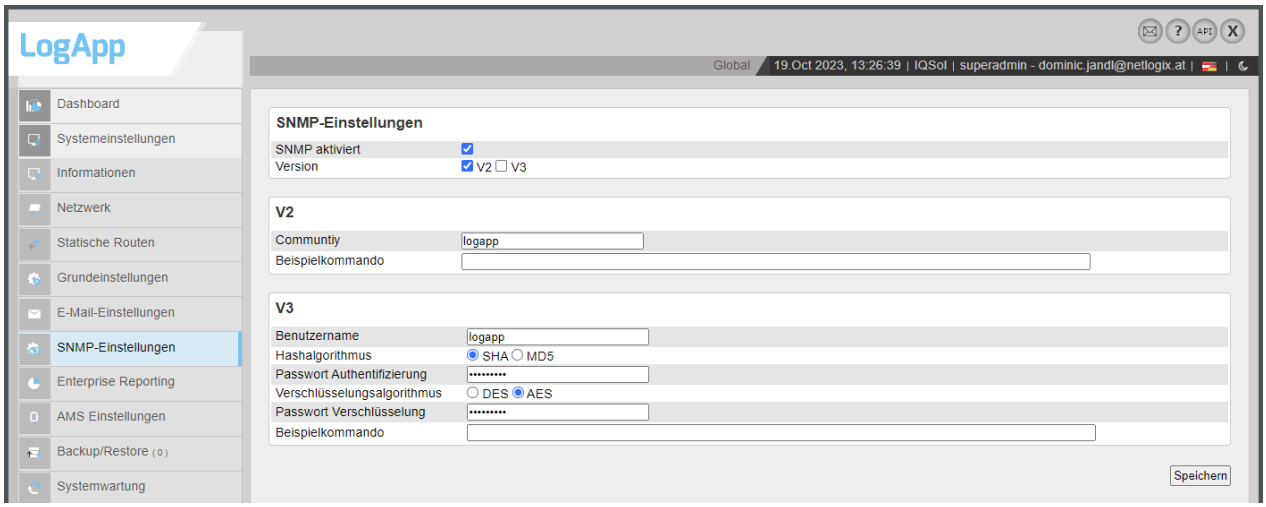

Abbildung 51: SNMP Einstellungen

Die verfügbaren OIDs, die über SNMP abgefragt werden können, werden im Anhang

(Black und Whitelist bei Fileintegritymonitoring

Filter bei Black und Whitelists funktionieren beim Fileintegritymonitoring gleich, nur ist das Ergebnis ein anderes. Bei einem Match bei der Blacklist wird nicht gescanned, bei der Whitelist wird nur gescanned wenn ein Match da ist.

Filter können absolut (C:\Windows\System32) oder relativ zu den in den Pfaden definierten Pfaden angegeben werden. So erzielt schlussendlich ein Filter „System32“, bei einem definierten Pfad von „C:\Windows“ die gleiche Wirkung wie ein Filter „C:\Windows\System32“. Wird ein relativer Filter verwendet, so gilt dieser bei jedem Pfad. Sollten also bei einer ConfigGruppe die Pfade C:\Windows\System32 und C:\Program Files (x86)\ definiert sein, so erzielt ein Filter System32 die gleiche Wirkung wie zwei Filter „C:\Windows\System32“ und „C:\Program Files (x86)\System32“.

Unterschiede zwischen Filter auf Files und Directories

Files

Files können (egal ob absolut oder relativ) mit ganzen Filenamen (authentication.dll bzw C:\Windows\System32\authentication.dll) oder mit einer Wildcard angegeben werden (*.dll bzw. C:\Windows\System32*.dll). Bei einer Wildcard ist es dabei egal ob der ganze Pfad angegeben wird. So kommt es bei einem File „C:\Windows\System32\Auth\authentication.dll“ sowohl bei einem Filter „*.dll“ als auch bei einem Filter „C:\Windows\System32\Auth*.dll“ zu einem Match.

Directories

Im Gegensatz zu den Files gibt es bei Directories keine Wildcard. Der Name des Directories muss (egal ob absolut oder relativ) ganz übergeben werden. Z.b. C:\Windows\System32 oder System32

Beispiele

Pfade	C:\Windows\
Blacklist	System32
Ergebnis	
In diesem Beispiel wird das gesamte „C:\Windows“ Directory gescanned, mit der Ausnahme des Directories „C:\Windows\System32“. Ein File welches den Pfad „C:\Windows\System32.dll“ aufweißt würde jedoch gescanned werden.	

Tabelle 35: Beispiel 1 FIM Black/Whitelist

Pfade	C:\Windows\
Blacklist	C:\Windows\System32
Ergebnis	
Entspricht dem vorangegangenen Beispiel	

Tabelle 36: Beispiel 2 FIM Black/Whitelist

Pfade	C:\Windows\ C:\Temp\
Blacklist	*.dll
Ergebnis	
Die Pfade „C:\Windows\“ und „C:\Temp\“ werden gescanned, jeodch werden alle .dll files ausgenommen.	

Tabelle 37: Beispiel 3 FIM Black/Whitelist

Pfade	C:\Windows\ C:\Temp\
Blacklist	C:\Temp*.dll
Ergebnis	
Die Pfade „C:\Windows\“ und „C:\Temp\“ werden gescanned, jeodch werden alle .dll files im Directorie C:\Temp\ ausgenommen.	

Tabelle 38: Beispiel 4 FIM Black/Whitelist

SNMP Abfragen mittels OID) dargestellt.

5.2.8 Enterprise Reporting

Mit der Option „ERS Service aktiv“ kann die LogApp für die Verwendung mit einem Enterprise Reporting Server (ERS) vorkonfiguriert werden. Dabei kann, falls mehrere Interfaces konfiguriert sind, zwischen diesen ausgewählt werden. Das Aktivieren des ERS Service erfordert einen Neustart der LogApp.

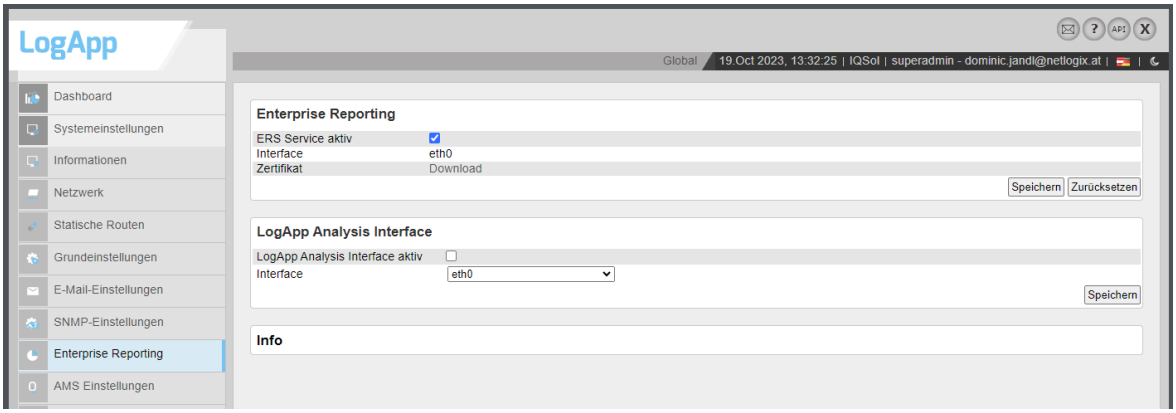

Abbildung 52: Enterprise Reporting

Nach dem Neustart kann ein SSL Zertifikat heruntergeladen werden, das für die Installation des Enterprise Reporting Servers erforderlich ist.

Um einen ERS zu installieren, lesen Sie bitte das Handbuch „ERS_Installationsanleitung“.

5.2.9 LogApp Analysis Interface

Wird das LogApp Analysis Interface aktiviert, so können ähnlich einer Installation von Opensearch, Queries an eine REST Schnittstelle abgesetzt werden, um Suchen, Aggregationen oder ähnliches zu bewerkstelligen.

Die Schnittstelle ist bei Aktivierung auf dem Port 9400 auf dem gewählten Interface zu erreichen.

Nach der Aktivierung kann ein Archiv mit einem Zertifikat und einem Schlüssel heruntergeladen werden, welche zur Authentifizierung benötigt werden.

!Achtung! Da dieses Zertifikat selbstsigniert ist, ist dies bei den Abfragen zu berücksichtigen.

Beispiel:

Mit diesem Beispiel lassen sich alle Indizes einer LogApp anzeigen:

```
curl --insecure -X GET
"https://10.100.181.240:9400/_cat/indices/*?v=true&s=index&pretty" --cert
/AnalysisInterfaceCerts/analysis-interface-client.crt --key
/AnalysisInterfaceCerts/analysis-interface-client.key
```

Für die Verwendung des LogApp Analysis Interface müssen genügend Analysis Interface Agenten Lizenzen vorhanden sein (siehe Lizenz). Sollten nicht genügend Lizenzen vorhanden sein, so lässt sich das Interface nicht aktivieren. Sollte es bereits aktiv sein und es liegt eine Unterlizensierung vor, so wird das Interface gestoppt und wieder gestartet, wenn genügend Lizenzen vorhanden sind.

5.2.10 AMS Einstellungen

In den AMS Einstellungen kann der IQSol Alert Messaging Server zur weitergehenden Alarmierung per SMS oder Voice angebunden werden.

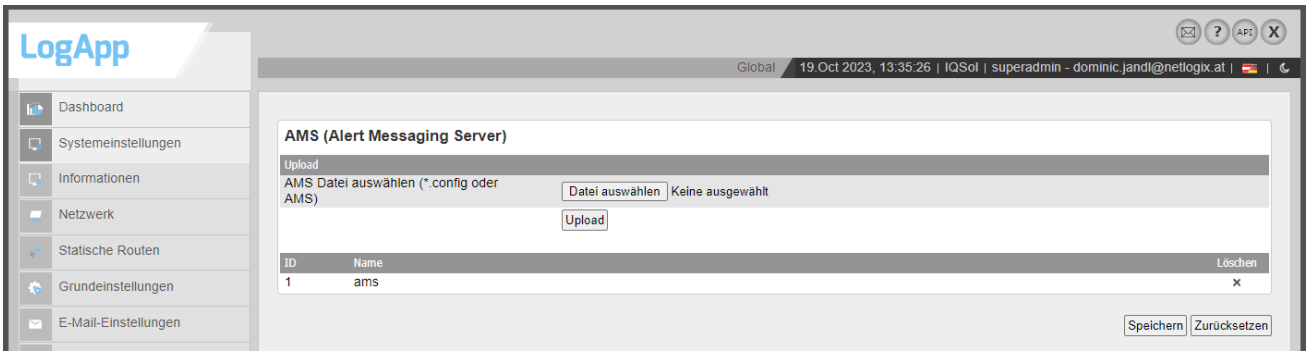

Abbildung 53: AMS (Alert Messaging Server) Einstellungen

Für die Anbindung des AMS müssen der in Verwendung befindliche AMS Client sowie die für die LogApp erstellte Konfigurationsdatei gespeichert werden. Beide Files können über das AMS Management Interface bezogen werden.

Entsprechend den Einstellungen ergibt ein weitergeleiteter Alarm folgende Ergebnisse:

- Email:
  Betreff: [DATUM UHRZEIT] AMS Alert ([AMSALERTID])
  Nachrichtentext: [[LOGAPP_ALERT_ID] - [LOGAPP_ALERT_PRIORITY]] [LOGAPP_ALERT_DESCRIPTION] Devices: [LOGAPP_ALERT_AFFECTED_DEVICES] , LogApp IP: [LOGAPP_IP]
  Beispiel:

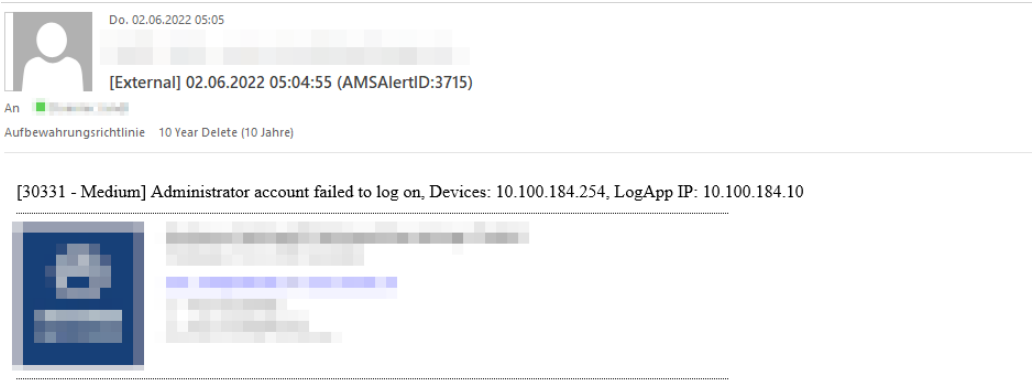

Abbildung 54: AMS EMail

- SMS:
  (AMSAlertID:[AMS_ALERT_ID]) [DATUM UHRZEIT], < [LOGAPP_ALERT_ID] - [LOGAPP_ALERT_PRIORITY] > [LOGAPP_ALERT_DESCRIPTION] Devices: [LOGAPP_ALERT_AFFECTED_DEVICES], LogApp IP: [LOGAPP_IP]
  Beispiel: (AMSAlertID:228) 21.06.2019 07:43:34, <542 – High> An Administrator failed to log on, Devices: LADevHost03, LogApp IP: 10.100.185.10

- Voice:
  Bei der Voicealarmierung wird ein Anruf getätigt, welcher es ermöglicht den Alarmtext anzuhören, welcher der Alarmbeschreibung entspricht die durch Text-To-Spech verarbeitet wird, und den Alarm zu bestätigen

5.2.11 Backup/Restore

In der Zentralkonsole können Backups erstellt und wiederhergestellt werden. Backups können durch einen Klick auf den „Backup“-Button, oder automatisiert in einem hinterlegten Intervall, erstellt werden. Regelmäßige, automatische Backups können hier auch konfiguriert werden. Es wird empfohlen, Backups herunterzuladen und extern abzulegen. Backups beinhalten alle Einstellung der LogApp, aber keine Ereignisse und Alarme. Backups sind mit einer Demolizenz nicht möglich.

Sämtliche Zertifikate (Webseite, Verbindungsschlüssel) müssen über ein eigenes Backup gesichert werden. Dies geschieht über den Button „LogApp Schlüssel exportieren“.

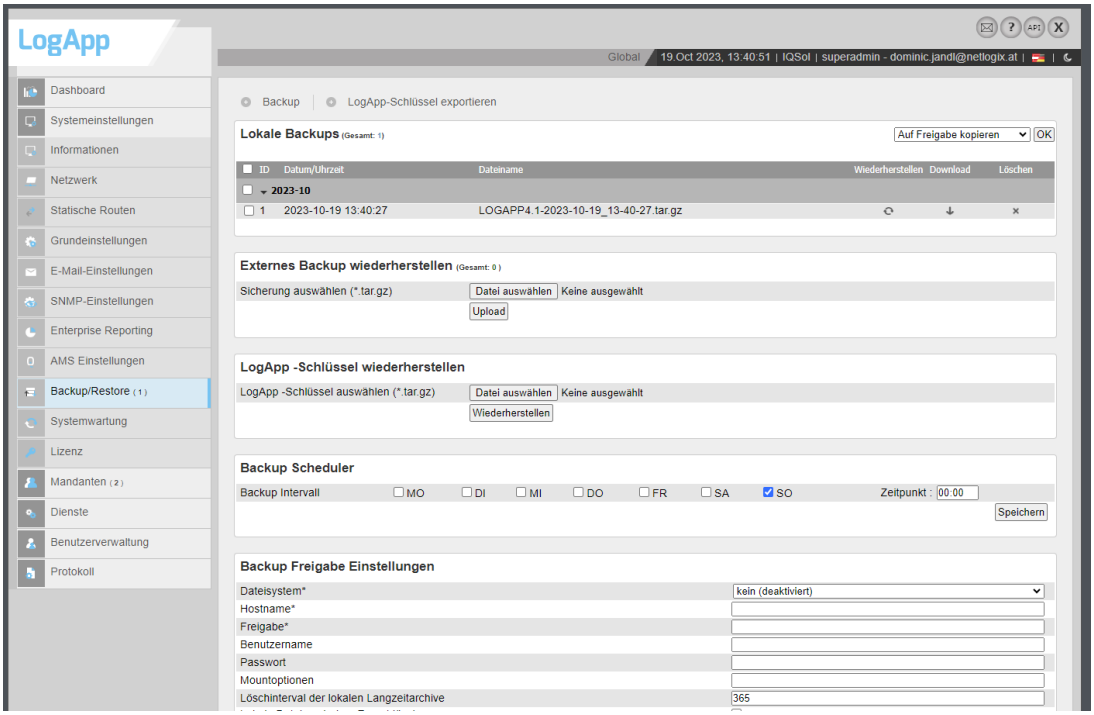

Abbildung 55: Backup und Restore

Lokale Backups auf der LogApp können über die entsprechenden Buttons wiederhergestellt, heruntergeladen oder gelöscht werden. Extern abgelegte Backups müssen vor einer Wiederherstellung hochgeladen werden.

Der Name eines Backups sollte nicht verändert werden. Ein Präfix (z.B.: DMZ_LOGAPP3.6-2021-05-11_08-31-11.tar.gz) ist erlaubt. Weitere Änderungen wie zum Beispiel Änderung der Dateiendung oder Änderungen in der Mitte des Dateinamens werden nicht unterstützt.

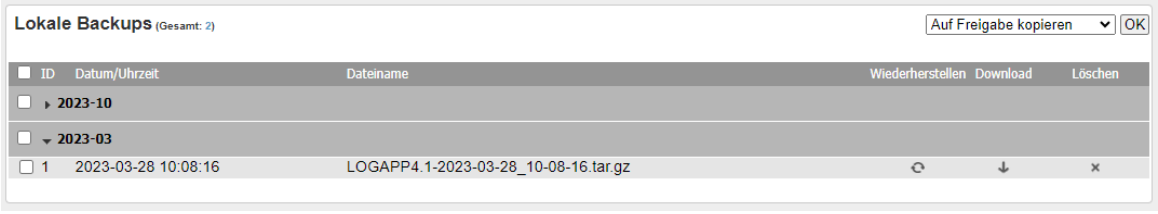

Abbildung 56: LogApp Backups

Im Falle eines Defektes wird empfohlen, die Ersatz-LogApp mit den gleichen Netzwerkeinstellungen aufzusetzen und im Anschluss ein Backup wiederherzustellen. LogAgents können nach der Wiederherstellung eines Backups wieder eine Verbindung zur LogApp herstellen und den Betrieb fortsetzen. Wenn nach der Erstellung des Backups LogAgents angelegt wurden, müssen diese neu installiert werden.

Im Falle einer Wiederherstellung können sowohl alle Einstellungen, als auch nur Ausgewählte Teile dieser wiederhergestellt werden.

Es kann für die Backups auch ein SMB-Share angegeben werden.

Option	Beschreibung
Backup Freigabe Einstellungen	
Dateisystem	Auswahl des Dateisystems für das Langzeitarchiv, entweder SMB/CIFS-Freigabe oder lokal
Hostname	FQDN (Fully Qualified Domain Name) oder IP des File Servers
Freigabe	Freigabename auf dem File Server
Benutzername	Benutzername für die Authentifizierung
Passwort	Passwort für die Authentifizierung
Mountoptionen	Optionen, welche dem Linux Mount Befehl mitgegeben werden können, z.B. sec=ntlmv2i, DOMAIN='example, vers=2.0'. Details entnehmen Sie dazu den mount man pages. Zum Testen kann folgender Mount-Befehl verwendet werden (mit oben genannten Optionen): `sudo USER='YYY' PASSWD='XXX' mount -o sec=ntlmv2i,DOMAIN='ZZZ',uid=www-data,gid=www-data -t cifs //192.168.205.131/laa/ /archive/2/ 2>&1`
Lokale Datei nach dem Export löschen	Aktivieren, um das Archiv nur auf dem externen Share abzulegen (empfohlen)

Tabelle 6: Einstellungen eines Backup-Shares

5.2.12 Systemwartung

Unter dem Menüpunkt „Systemwartung“ können verfügbare Updates installiert werden. Updatepakete können von iQSol oder einem Partner von iQSol bezogen und hochgeladen werden.

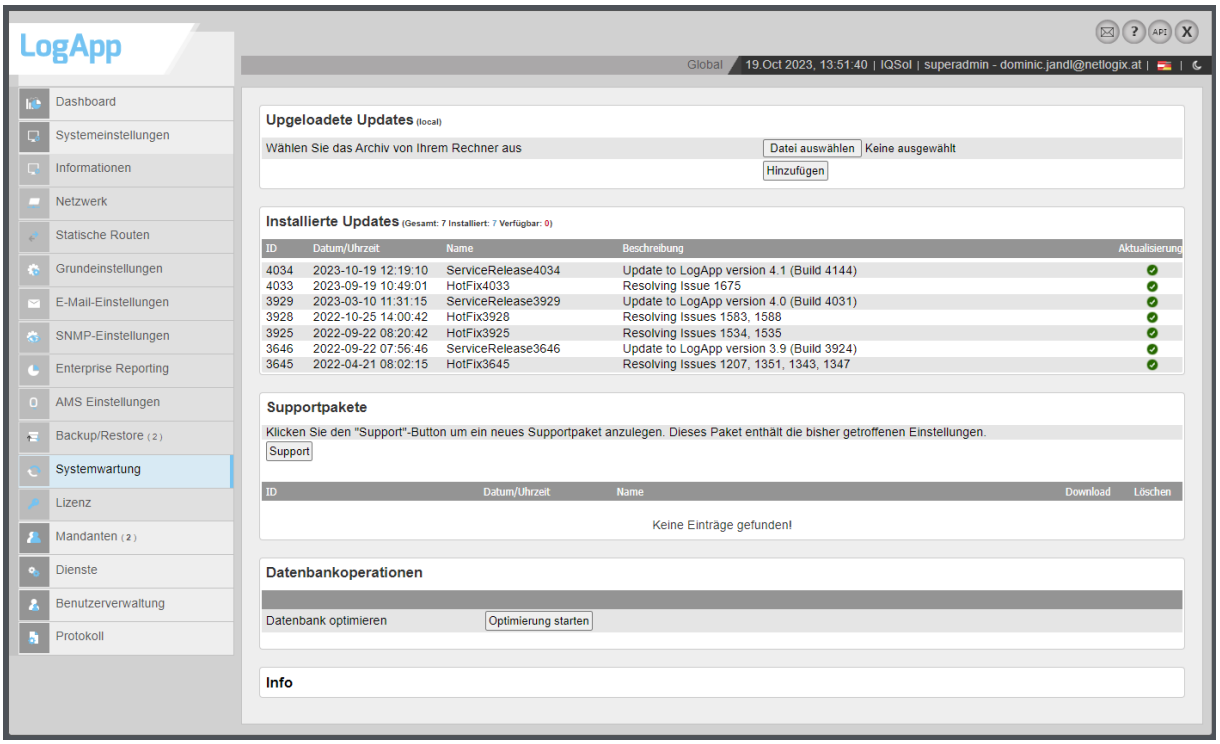

Abbildung 57: Updates

Nach dem Hochladen eines Updatepaketes kann das Update installiert werden. Es besteht auch die Möglichkeit, Updates hinzuzufügen und diese erst zu einem späteren Zeitpunkt zu installieren. Ob ein Update installiert wurde, ist erkennbar an dem grünen Hacken der sich neben der Updatebeschreibung befindet. Ist ein Update nur hinzugefügt und noch nicht installiert worden, so erscheint ein Pfeilkreis. Mit einem Klick auf diesen wird das Update installiert.

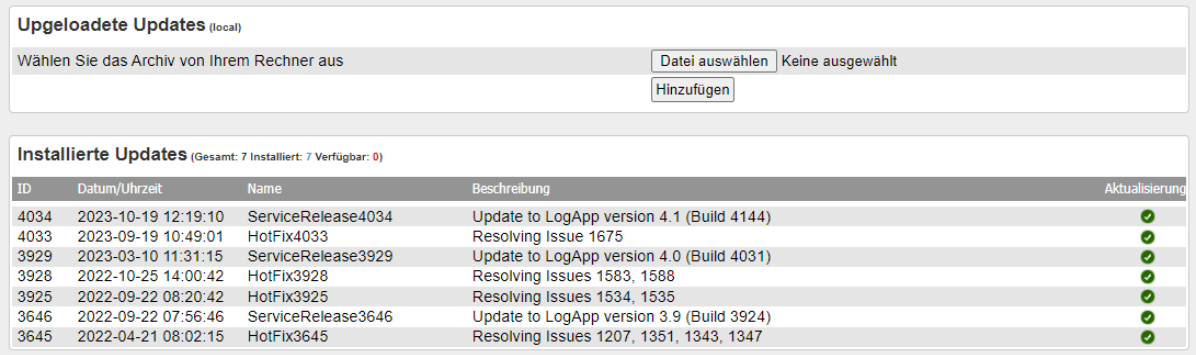

Abbildung 58: Installierte Updates

Updates werden als kumulative Updatepakete ausgeliefert, das heißt jedes Update beinhaltet auch alle vorangegangenen Updates für die jeweilige LogApp Version.

Im unteren Teil der Seite können Supportpakete erstellt werden. Supportpakete enthalten alle wichtigen Einstellungen und Logdateien und sollten im Supportfall an den Support übermittelt werden, um die Fehlersuche zu erleichtern. Supportpakete enthalten keine Events, Alarme oder Benutzerdaten.

Abbildung 59: Supportpakete

Die Funktion “Datenbank optimieren" ist ein nützliches Werkzeug für die Datenbankwartung. Mit dieser Funktion können Sie die Tabellen in Ihrer MySQL-Datenbank (Tablespace) optimieren, um die Leistung und Effizienz zu verbessern. Es wird empfohlen, die Agenten vor Beginn der Optimierung in den Heartbeatonly-Modus zu versetzen.

5.2.13 Lizenz

Im Menüpunkt „Lizenz“ muss ein Lizenzfile, welches Sie von iQSol oder einem Reseller bekommen, hochgeladen werden. Standardmäßig ist eine 30-Tage-Demolizenz vorinstalliert.

Folgende Lizenzen werden unterschieden:

Lizenz	Beschreibung
LogApp – Basislizenzen	
LogApp Basislizenz	Funktionsdauer der LogApp in Tagen
LogApp Wartungslizenz	Wartungszeitraum für LogApp in Tagen. Während der Wartungsdauer können Updates bezogen werden.
Log Quellen – Modul	
Server Agenten	Anzahl der LogAgents für Server
Windows Client Agenten	Anzahl der LogAgents für Windows, welche nur die Standard Windows Eventlogs auslesen können
Netzwerkgeräte	Anzahl der Syslog Quellen, die Syslog Nachrichten senden können.
Enterprise Reporting Agenten	Anzahl der Log Quellen, deren gesammelte Daten vom Enterprise Reporting Server berücksichtig werden.
Analysis Interface Agenten	Diese Lizenz gibt die Höchstanzahl an Mandantenübergreifenden Agenten an, welche auf der LogApp installiert sein dürfen um das Analysis Interface zu verwenden. Diese Lizenz kann und muss keinem Mandanten zugewiesen werden.

Tabelle 7: Lizenzen

Verfügbare LogAgent- Lizenzen müssen im mittleren Teil der Seite auf die vorhandenen Mandanten verteilt werden. Mandanten können maximal die Anzahl der zugewiesenen LogAgents anlegen.

Basis- und Wartungslizenzen gelten für das gesamte Produkt und müssen nicht auf Mandanten verteilt werden.

Nach Ablauf der Wartungslizenz können keine Produktupdates mehr bezogen werden. Läuft die Basislizenz ab, werden wesentliche Teile der Benutzeroberfläche eingeschränkt. Es wird empfohlen, ablaufende Lizenzen rechtzeitig zu verlängern.

Abbildung 60: LogApp Lizenz

Lizenzreport

Als letzter Punkt kann ein Lizenzreport generiert werden.

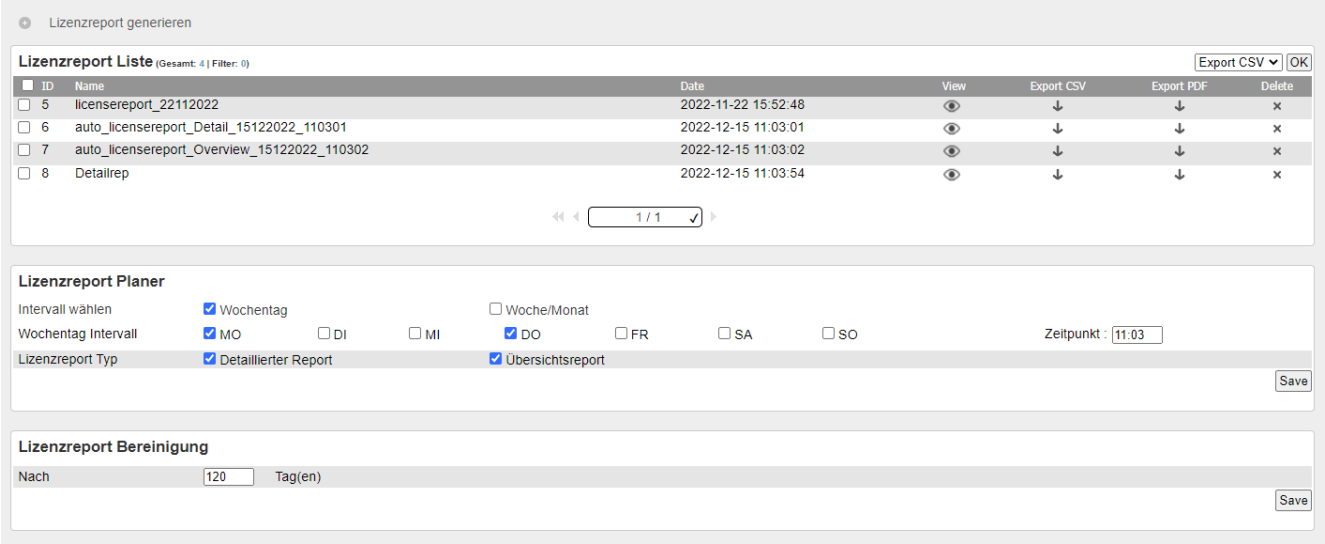

Abbildung 61: Erweitertes Lizenzreporting

Im Fenster „Lizenzreport generieren“ muss dem Lizenzreport ein Name gegeben werden, ein Lizenzreportstyp ausgewählt werden und es muss gewählt werden, ob der Lizenzreport auf der LogApp gespeichert werden soll oder nicht.

Es stehen zwei Lizenzreporttypen zur Auswahl:

Lizenzreporttyp	Beschreibung
Detaillierter Report	Die zugewiesenen Lizenzen sowie die aktiven (tatsächlich Verbrauchten) Lizenzen werden pro Mandant aufgelistet.
Übersichtsreport	Alle Lizenzen der LogApp werden aufgelistet.

Tabelle 8: Lizenzreporttypen

Die gespeicherten Lizenzreports können in der Lizenzreport Liste verwaltet werden. Hier können Sie die Lizenzreports im Browser ansehen, als CSV oder PDF exportieren und auch löschen.

Im Lizenzreport-Planer können Sie die Erstellung von Lizenzreports automatisieren. Wählen Sie dazu das gewünschte Intervall, in dem die Lizenzreports erstellt werden sollen, und wählen Sie die Lizenzreporttypen, die automatisch erstellt werden sollen.

Es stehen zwei Intervalltypen zur Auswahl:

Intervalltyp	Beschreibung
Wochentag	Hier wählen Sie die Wochentage aus und legen die Uhrzeit fest, zu der die Lizenzreports erstellt werden sollen. (Format der Uhrzeit: HH:mm)
Woche/Monat	Hier können Sie auswählen, ob die Lizenzreports am ersten/letzten Tag der Woche oder des Monats erstellt werden sollen.

Tabelle 9: Intervalltypen

Bei Lizenzreport Bereinigung können Sie eine Löschfrist für die gespeicherten Lizenzreports festlegen. Hier geben Sie an, nach wie vielen Tagen die gespeicherten Lizenzreports automatisch gelöscht werden sollen. D.h. die Lizenzreports werden x Tage nach dem Erstellungsdatum gelöscht. Wenn Sie die Bereinigung von Lizenzreports nicht aktiviert möchten, stellen Sie 0 Tage ein.

5.3 Mandanten

In den Mandanteneinstellungen können Mandanten angelegt oder bearbeitet werden. Klicken Sie auf den Button „Mandant hinzufügen“ um einen neuen Mandant anzulegen.

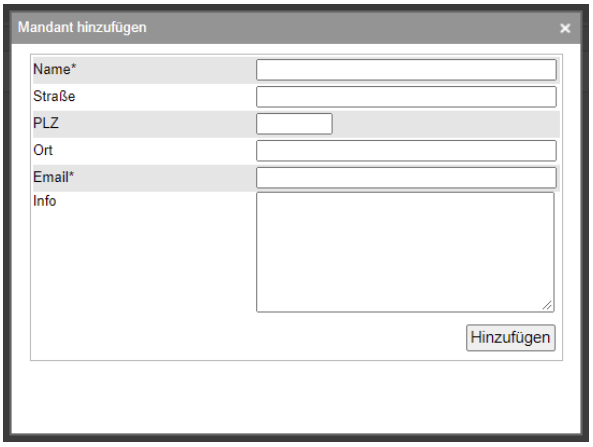

Abbildung 62: Mandant anlegen

Für neue Mandanten muss mindestens ein Name und eine E-Mail-Adresse für den admin-Account angegeben werden. Das Standardpasswort für den Account „admin“ des neuen Mandanten lautet „Admin1“. Das Passwort sollte **umgehend** geändert werden. Neu erstellten Mandanten sind keine Lizenzen zugeordnet.

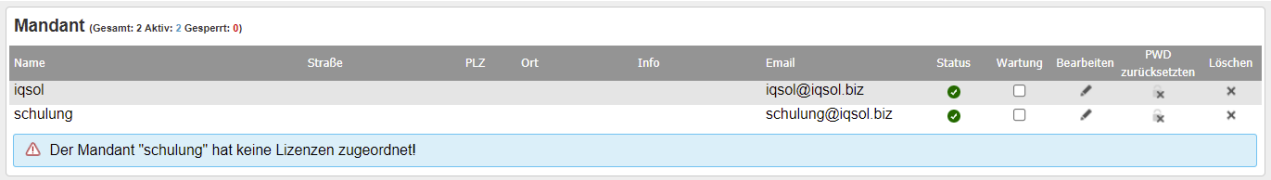

Abbildung 63: Mandanten

Mandanten können über die Funktionen in der Listenansicht bearbeitet werden. Mit dem „Status“-Button können Mandanten deaktiviert oder wieder aktiviert werden. Benutzer von deaktivierten Mandanten können sich nicht an der LogApp anmelden. Mit der Wartungs-Checkbox können Mandanten in den Wartungsmodus geschaltet werden. In diesem Modus werden keine Alarme generiert.

5.4 Dienste

Die zentralen LogApp-Dienste können vom Superadmin gestartet, gestoppt oder neugestartet werden. Das „Status“-Symbol zeigt an, ob der Dienst läuft.

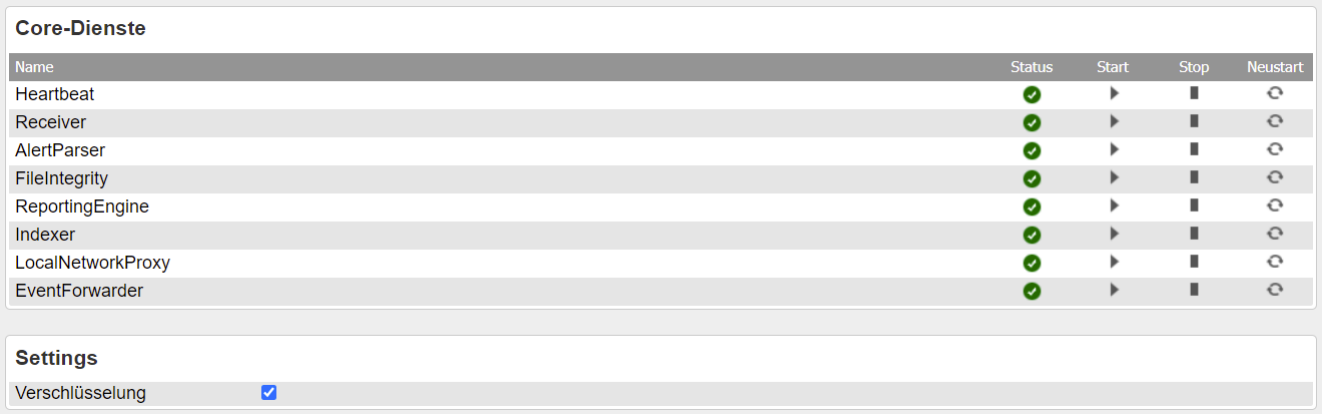

Abbildung 64: LogApp Dienste

Folgende Dienste sind für den ordnungsgemäßen Betrieb der LogApp notwendig:

Lizenz	Beschreibung
Core-Dienste	
Heartbeat	Der Heartbeat nimmt Heartbeat-Meldungen von LogAgents entgegen, um so den Status der LogAgents zu prüfen. Bei Konfigurationsänderungen wird den LogAgents vom Heartbeat-Dienst eine neue Konfiguration bereitgestellt.
Receiver	Der Receiver nimmt Events von LogAgents über eine verschlüsselte Verbindung entgegen.
AlertParser	Der AlertParser prüft alle eingehenden Events gegen die angelegten Alarmregeln und erzeugt ggf. einen Alarm.
FileIntegrity	Der File Integrity-Dienst kommuniziert direkt mit dem Agent und erzeugt ein Event, wenn eine Änderung an einer Datei festgestellt wird.
ReportingEngine	Die Reporting Engine sammelt Daten für Reports und Report Widgets.
Indexer	Der Indexer indiziert alle gesammelten Ereignisse und stellt sie für die Anzeige und Suche zur Verfügung.
LocalNetworkProxy	Der lokale Network-Proxy kann Syslog-Nachrichten und SNMP-Traps direkt auf der LogApp empfangen.
EventForwarder (nur bei aktiviertem EventForwarding sichtbar)	Der EventForwarder leitet Events, falls eine Weiterleitung pro Mandanten aktiviert ist, an eine weitere LogApp weiter. Dieser Dienst ist in der Grundeinstellung deaktiviert.

Tabelle 10: LogApp Dienste

Im Abschnitt Settings kann die Verschlüsselung der Kommunikation zwischen Agenten zur LogApp (de)aktiviert werden.

5.5 Benutzerverwaltung

Siehe Kapitel 4 - Allgemeine Einstellungen.

5.6 Protokoll

Unter dem Menüpunkt „Protokoll“ werden Systemereignisse und sicherheitsrelevante Vorfälle die LogApp selbst betreffend aufgezeichnet.

Das Protokoll ist in folgende Kategorien unterteilt:

Modus	Beschreibung
Mandanten	Änderungen an Mandanten
System	Änderungen in Systemeinstellungen
Benutzer	Änderungen in der Benutzerverwaltung / Benutzerverhalten
Services	Statusmeldungen der Dienste
API	Statusmeldungen der REST API, wie Auhtentifizierungsversuche, etc.

Tabelle 11: Protokollkategorien

Protokolleinträge werden jeweils mit Datum/Uhrzeit, einer Beschreibung, einem Benutzer und eine Quell-IP angezeigt. Der Benutzer ist entweder der angemeldete Benutzer mit seiner Client-IP oder der Benutzer „System“ mit der IP 127.0.0.1. Mit dem „Details“-Button können weitere Details zu den Ereignissen eingesehen werden.

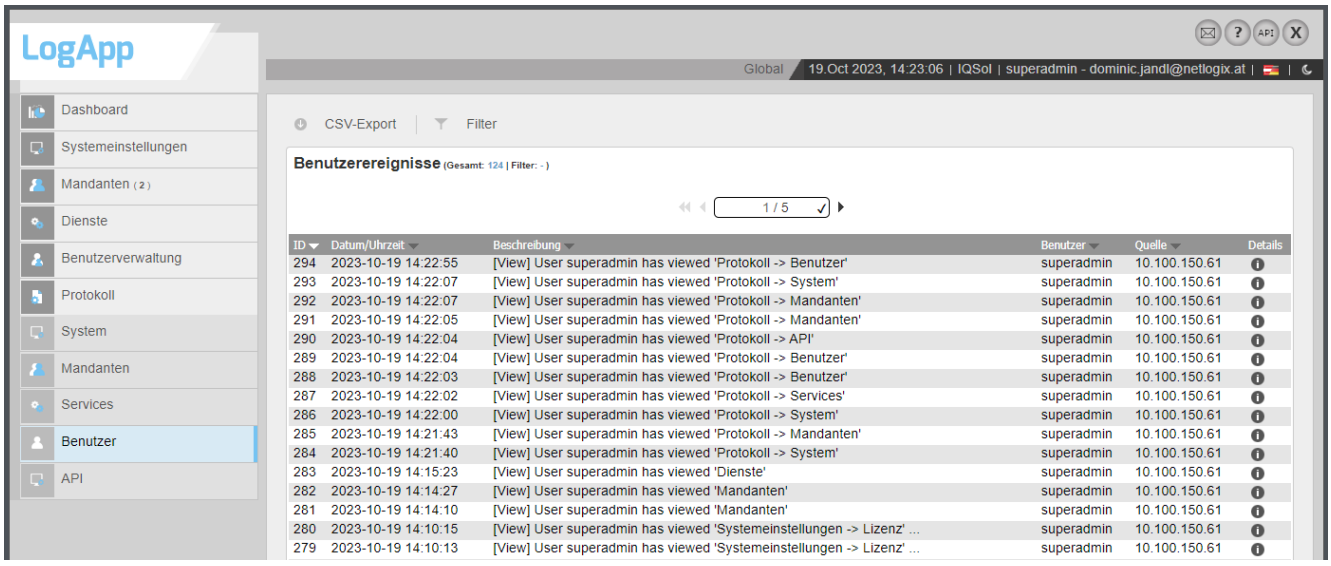

Abbildung 65: Benutzerprotokoll

Der „Filter“-Button im oberen Bereich der Seite ermöglicht das Suchen in den Protokolleinträgen. ID, Datum/Uhrzeit, Beschreibung, Benutzer und Quell-IP können beliebig eingeschränkt werden, um nach bestimmten Ereignissen zu suchen.

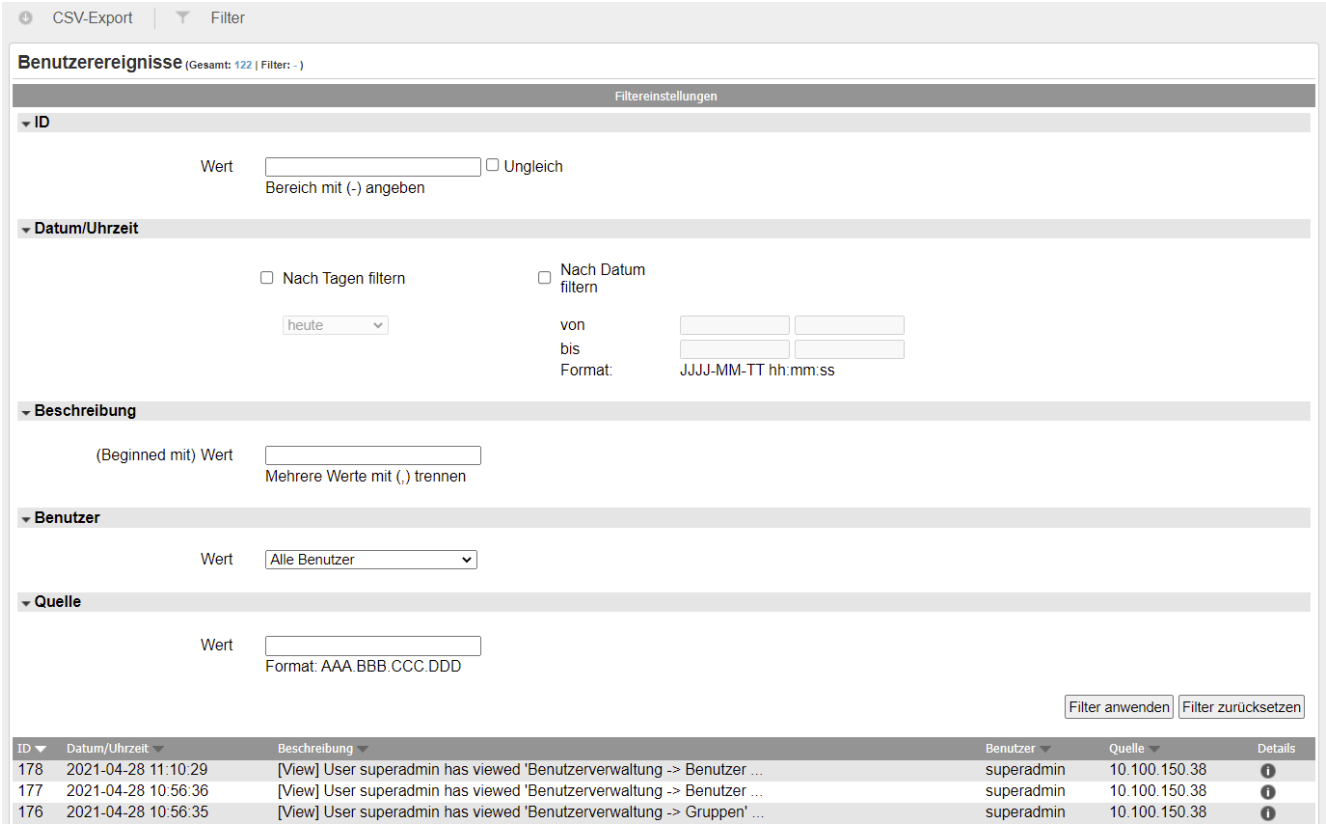

Abbildung 66: Filter

5.7 Zugriff via CLI (Command Line Interface)

Der „Superadmin“ hat neben der zentralen Konfiguration über die GUI auch die Möglichkeit, verschiedene Befehle über die CLI auszuführen. Der Zugriff auf die CLI erfolgt über das Management-Interface per SSH. Unter Windows kann dafür entweder das Windows Terminal oder das Programm PuTTY verwendet werden. Der Login erfolgt mit dem User „Superadmin“ und dem zugehörigen Passwort. Um alle verfügbaren Kommandos aufzulisten oder Hilfe zu einem Befehl zu erhalten, kann man die Zeichen „?“, „h“ oder „help“ verwenden.

Abbildung 67: Zugriff via CLI

Folgende Kommandos stehen zur Verfügung:

Kommando	Beschreibung	Verwendung
	HDDManagement	
	Befehle zur Erweiterung der virtuellen Festplatte (nur für LogApp VM). Siehe Anhang „Vergrößerung der virtuellen Festplatte“. **Achtung:** die Anwendung dieser Befehle wird nur in Rücksprache mit dem IQSOL Support empfohlen!	
Cfdisk	Befehl zur Verwaltung von Festplattenpartitionen mit dem Dienstprogramm cfdisk.	cfdisk [existing HDD]
Fdisk	Befehl zum Auflisten der Partitionstabelle für alle oder bestimmte Festplatten mit dem Dienstprogramm fdisk.	fdisk -l [disk]
LvDisplay	Befehl zur Anzeige der Attribute eines logischen Volumes.	lvdisplay
LvExtend	Befehl zum Erweitern eines logischen Volumes.	lvextend -L+[number of gb to extend]G /dev/mapper/vg_db-var
Pvcreate	Befehl zum Initialisieren eines physischen Volumes für die Verwendung durch LVM.	pvcreate [partition]
PvScan	Befehl zum Scannen aller Festplatten nach physischen Datenträgern.	pvscan
Resize2fs	Befehl zur Größenänderung des Dateisystems auf einem logischen Volume.	resize2fs /dev/mapper/vg_db-var
VgDisplay	Befehl zur Anzeige der Attribute von Volume-Gruppen.	vgdisplay
VgExtend	Befehl zum Hinzufügen physischer Volumes zu einer Volume-Gruppe.	vgextend vg_db [physical volume]
	Network	
Arp	Befehl zur Anzeige der ARP-Tabelleneinträge.	arp
Dig	Befehl zur Durchführung einer DNS-Suche.	dig [Hostname]
Hostname	Befehl, um den Hostnamen des Systems anzuzeigen.	hostname
Ifconfig	Befehl zum Anzeigen oder Konfigurieren von Netzwerkschnittstellenparametern.	ifconfig [network interface]
Netstat	Befehl zur Anzeige aller offenen Ports und der zugehörigen Netzwerkstatistiken.	netstat
Nslookup	Befehl zur Durchführung einer DNS-Suche für einen bestimmten Hostnamen.	nslookup [Hostname]
Ntpdate	Befehl zum Einstellen von Datum und Uhrzeit über NTP (Network Time Protocol).	ntpdate

Ping	Befehl zur Überprüfung der Erreichbarkeit eines Hosts im Netz.	ping [Host]
Route	Befehl zur Anzeige der Routing-Tabelle des Systems.	route
Tcpdump	Befehl zum Erfassen und Anzeigen von Netzwerkverkehrspaketen.	tcpdump [interface] [port]
Telnet	Befehl zur Durchführung eines Telnet-Vorgangs zum Testen der Erreichbarkeit eines Servers.	telnet [IP] [PORT]
Traceroute	Befehl zum Verfolgen der Route, die Pakete zu einem Netzwerkhost nehmen.	traceroute [Host]
	OSManagement	
Date	Befehl zur Anzeige des aktuellen Datums und der Uhrzeit.	date
RaidStatus	Befehl, um den Status des RAID-Arrays zu überprüfen.	raidStatus
Reboot	Befehl zum Neustart des Systems.	reboot
Shutdown	Befehl zum Herunterfahren des Systems.	shutdown
TopCommand	Befehl zeigt eine Zusammenfassung des aktuellen Systemzustands an, einschließlich CPU-, Speicher- und Swap-Nutzung.	top
	LogAppSpecific	
ActivateSupportMode	Befehl zur Aktivierung des Unterstützungsmodus in der LogApp-Anwendung. **Achtung:** Nur Für Supportzecke des IQSOL Supports vorgesehen	activate_supportmode
DeactivateSupportMode	Befehl zum Deaktivieren des Unterstützungsmodus in der LogApp-Anwendung. **Achtung:** Nur Für Supportzecke des IQSOL Supports vorgesehen	deactivate_supportmode
Debug	Mit Hilfe des Befehls „debug“ können die Logeinstellungen verändert werden. Z.B.: debug true Dabei werden detailliertere Informationen für die unterschiedlichen Services in den Logfiles geschrieben. **Achtung:** Debug Modus nach Troubleshooting wieder auf „debug false“ setzten.	debug [show\set] [true\false]

Dblimits	Befehl zum Anzeigen/Setzen von Grenzwerten, ab denen die Services stoppen, um eine Überfüllung der HDD zu verhindern Mit dblimits view sieht man die aktuellen Werte. Diese kann man mit der Anzeige am Dashboard vergleichen und den Wert, der anschlägt, gegebenenfalls erhöhen. Die Grundeinstellungen sind: Minimaler freier Platz im EventDBFile: 10% (Minimaler Prozentsatz, welcher im Datebankfile frei sein muss, sollte ein Clientlimit schlagend werden (siehe unten unter ClientLimits)) Minimaler freier Platz in ibdata: 10% (Minimaler Prozentsatz, welcher im Datebankfile frei sein muss, sollte das Filelimit erreicht worden sein) ClientLimits Event file limit for Client1: 40% (Maximale Größe des DBfiles für den Mandanten 1) Geprüft wird, ob das Event-File Limit am Client erreicht ist. Wenn ja, dann wird geprüft ob in den beiden DB-Files (durch das Löschen von Events) eventuell schon wieder genug Platz frei ist, sodass das Event-File nicht mehr wachsen würde. Wenn alle drei Bedingungen nicht erfüllt sind, werden die Services gestoppt. Mit „dblimit change [parameter] [ClientID] [Maximal % disk usage]“ (z.B.) dblimits change eventfilelimit 1 80 kann man die Werte erhöhen. **Achtung:** die Änderung dieser Werte wird nur in Rücksprache mit dem IQSOL Support empfohlen!	dblimits [view\change] [eventfilelimit\freespacelimit] [value]
Indexer	Der IndexerCommand dient der Verwaltung und Konfiguration der Indexierungsmaschine. Mit diesem Befehl können zentrale Parameter der Indizierungsmaschine wie das Aktualisierungsintervall und die Heap-Größe direkt in den Konfigurationsdateien angepasst werden. Die Änderungen werden wirksam, wenn die Indizierungsmaschine manuell neu gestartet wird. **Achtung:** die Änderung dieser Werte wird nur in Rücksprache mit dem IQSOL Support empfohlen!	indexer set [refresh_interval|heapSize] [value]
InstallVmwareToolsCommand	Befehl zur Installation der VMware Tools.	install-vmware-tools
Log	Mit diesem Befehl können Protokolle für verschiedene Dienste verwaltet und angezeigt werden. Sie können die Logs einzelner Dienste einsehen, um detaillierte Informationen über deren Betrieb zu erhalten.	log [heartbeat] log [receiver] log [fim] log [localsyslogproxy] log [archive] log [logappparser] log [logappreportingengine] log [?]

Service	Befehl zur Steuerung verschiedener Dienste und ihrer Aktionen wie Start, Stopp, Neustart und Status	service [disableTLS1.0 |enableTLS1.0 |heartbeat |receiver |fim |reportingengine |parser |apache2 |rsyslog |localnetworkproxy |eventforwarder |indexer |db] [start|stop|restart|status]

Tabelle 12: CLI Befehle

6 Konfiguration eines Mandanten

6.1 Dashboard

Das Dashboard des Mandanten zeigt einen schnellen Überblick über das System und aktuelle Ereignisse. Es bietet auch die Möglichkeit, wichtige Analyse-Widgets einzublenden.

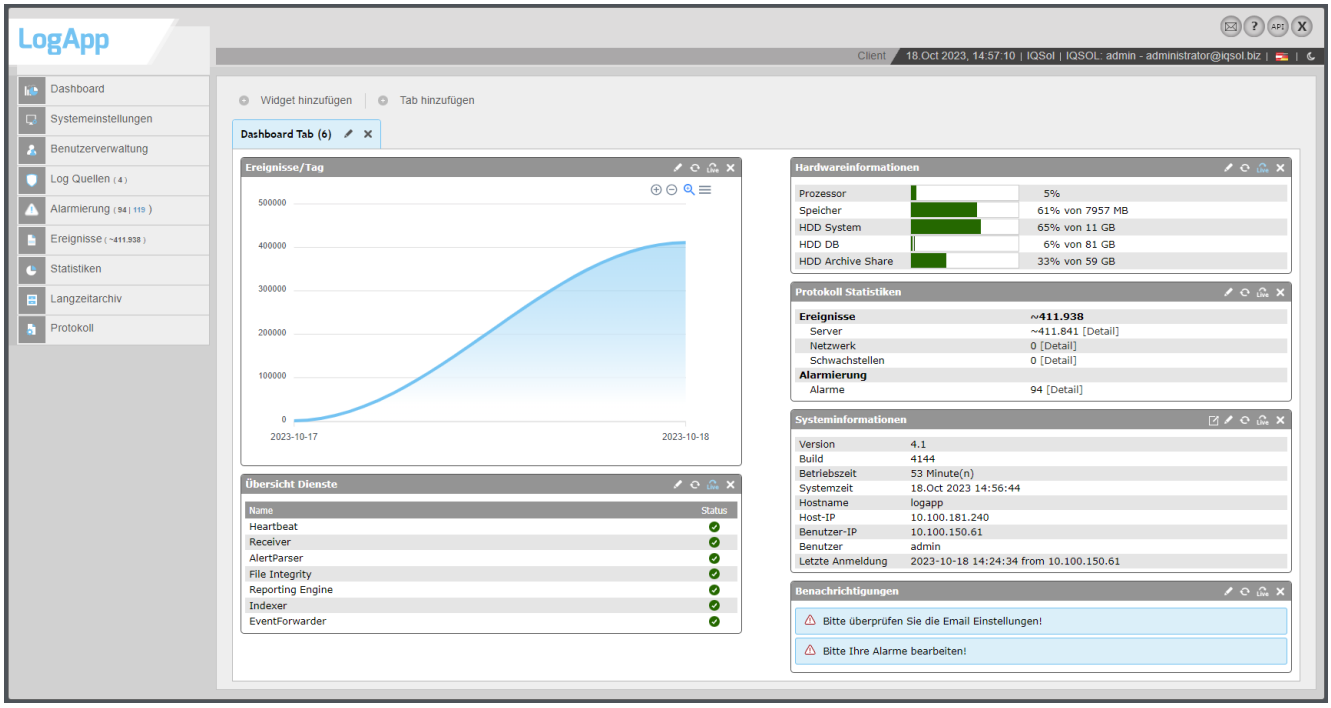

Abbildung 68: Dashboard Mandant

In folgender Tabelle werden sämtliche Widgets aufgelistet, welche im Mandantenbereich verfügbar sind.

Widget	Beschreibung
Hardwareinformation	Zeigt die Auslastung des Prozessors, des Hauptspeichers sowie der System- und Datenplatte.
Systeminformation	Allgemeine Informationen zum aktuellen System Dieses Widget besitzt einen Querlink. Im Header ist das „Springe zu -Icon“ zu finden. Wird dies geklickt, so gelangt man zum Menüpunkt „Systemeinstellungen“ -> „Informationen“
Benachrichtigungen	Hinweise zum Status des Systems wie z.B. der fehlenden Konfiguration eines E-Mail-Servers nicht erreichbaren Agenten. Bei nicht erreichbaren Agenten wird zusätzlich per E-Mail an den Mandanten-Administrator eine Warnung versandt **(die Konfiguration eines gültigen E-Mail-Servers sowie einer gültigen E-Mail-Adresse für den Administrator ist für diese Funktion unbedingt erforderlich!).** Wird auf eine Meldung geklickt, so gelangt man zum dazugehörigen Menüpunkt.

Protokoll Statistiken	Kennzahlen zum aktuell auftretenden Logvolumen und erzeugten Alarmen.
Report Widgets	Unter Statistiken angelegte Grafiken und Tabellen können am Dashboard angezeigt werden.
Übersicht Dienste	Auflistung der Dienste und deren Status.
Anmeldungsprotokoll	Auflistung der Anmeldungen
Überblick LogAgents	Auflistung aller LogAgents Dieses Widget besitzt einen Querlink. Im Header ist das „Springe zu -Icon“ zu finden. Wird dies geklickt, so gelangt man zum Menüpunkt „LogQuellen“ -> „LogAgents“
Überblick Netzwerkgeräte	Auflistung aller Netzwerkgeräte Dieses Widget besitzt einen Querlink. Im Header ist das „Springe zu -Icon“ zu finden. Wird dies geklickt, so gelangt man zum Menüpunkt „LogQuellen“ -> „Netzwerk“
Aktuelle Ereignisse	Auflistung der neuesten Ereignisse Dieses Widget besitzt einen Querlink. Im Header ist das „Springe zu -Icon“ zu finden. Wird dies geklickt, so gelangt man zum Menüpunkt „Ereignisse“ -> „Alle“

Tabelle 13: Widgets Dashboard Mandant

6.2 Systemeinstellungen

6.2.1 Informationen

Im Menüpunkt „Informationen“ werden allgemeine Systeminformationen und die Hardwareauslastung angezeigt. Wenn der verfügbare Speicherplatz auf der Datenbank-Partition knapp wird, sollten Sie die Archivierungszeiten verkürzen.

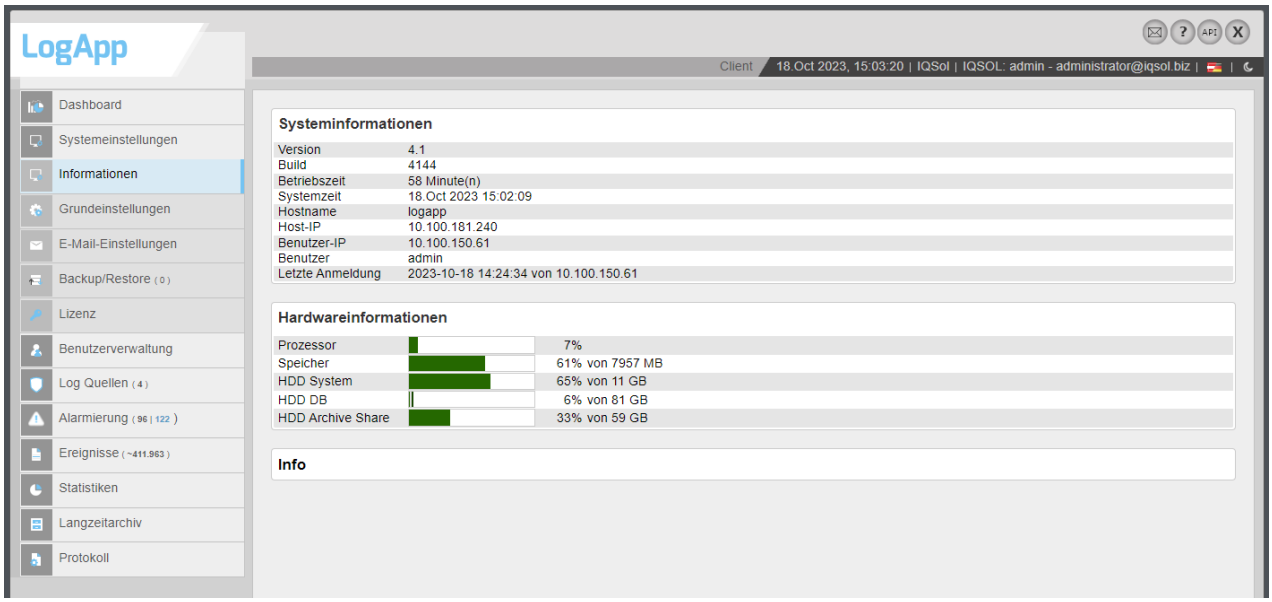

Abbildung 69: Systeminformationen

6.2.2 Grundeinstellungen

In den Grundeinstellungen der Mandantenkonsole können folgende wichtige Optionen festgelegt werden:

Option	Beschreibung
Allgemeine Einstellungen	
Aktualisierungsintervall	Intervall in Sekunden, in dem Listenansichten bei aktiviertem Live Update neu geladen werden.
Einträge pro Seite	Anzahl der Einträge pro Seite in Listenansichten
Alarm-Einträge pro Seite	Anzahl der Einträge pro Seite in der Alarmliste
Löscheinstellungen	
Alarme/Ereignisse	Anzahl der Tage, nach denen Alarme und Ereignisse ins Archiv verschoben werden.
Unvollständige Alarme	Anzahl der Tage, nach denen unvollständige Alarme ins Archiv verschoben werden.
Protokoll	Anzahl der Tage, nach denen Protokolleinträge ins Archiv verschoben werden.

Löschvorgang starten	Startet den Löschvorgang mit den oben eingegebenen Parametern. Dies ist nur möglich wenn kein anderer Archivjob oder Löschjob gestartet ist. Sollte dies der Fall sein, so kann dieser Job abgebrochen werden

Tabelle 14: Grundeinstellungen in der Mandantenkonsole

6.2.3 E-Mail Einstellungen

Siehe Kapitel 4 - Allgemeine Einstellungen.

Beim Auftreten von Alarmen werden bei aktiver globaler Alarmierung alle Benutzergruppen, oder anderenfalls nur die zuständige Benutzergruppe, per Mail verständigt.

Die genauen Alarmierungseinstellungen sind in Kapitel „7.1 Alarmierung“ beschrieben.

6.2.4 LDAP Einstellungen

Siehe Kapitel 4 - Allgemeine Einstellungen.

LDAP Benutzer können in der Benutzerverwaltung (Siehe Kapitel 4 - Allgemeine Einstellungen) importiert werden.

6.2.5 Backup/Restore Einstellungen

Neben den Backup Möglichkeiten in der Zentralkonsole können auch Backups pro Mandant erstellt und wiederhergestellt werden. Backups können durch einen Klick auf den „Backup“-Button oder automatisiert in einem hinterlegten Intervall, erstellt werden. Regelmäßige, automatische Backups können in den Grundeinstellungen (siehe 5.2.4 Grundeinstellungen) konfiguriert werden.

Es wird empfohlen, Backups herunterzuladen und extern abzulegen. Backups beinhalten alle Einstellung der LogApp, aber keine Ereignisse und Alarme. Ereignisse und Alarme sowie das Protokoll wird im Langzeitarchiv gespeichert (siehe Abschnitt 7.5).

Im Falle einer Wiederherstellung können sowohl alle Einstellungen, als auch nur Ausgewählte Teile dieser wiederhergestellt werden.

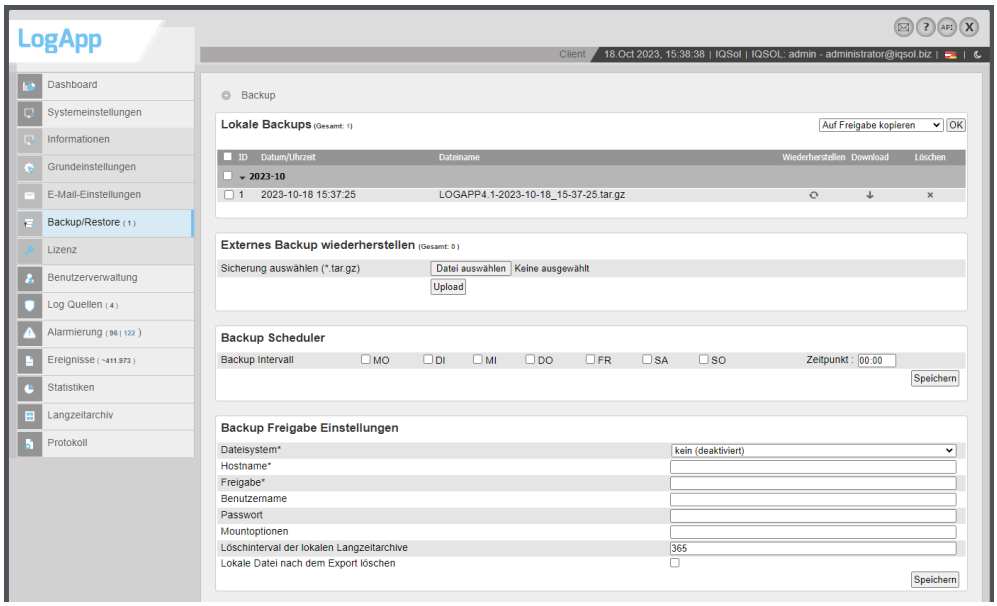

Abbildung 70: Backup/Restore pro Mandant

Lokale Backups auf der LogApp können über die entsprechenden Buttons wiederhergestellt, heruntergeladen oder gelöscht werden. Extern abgelegte Backups müssen vor einer Wiederherstellung hochgeladen werden.

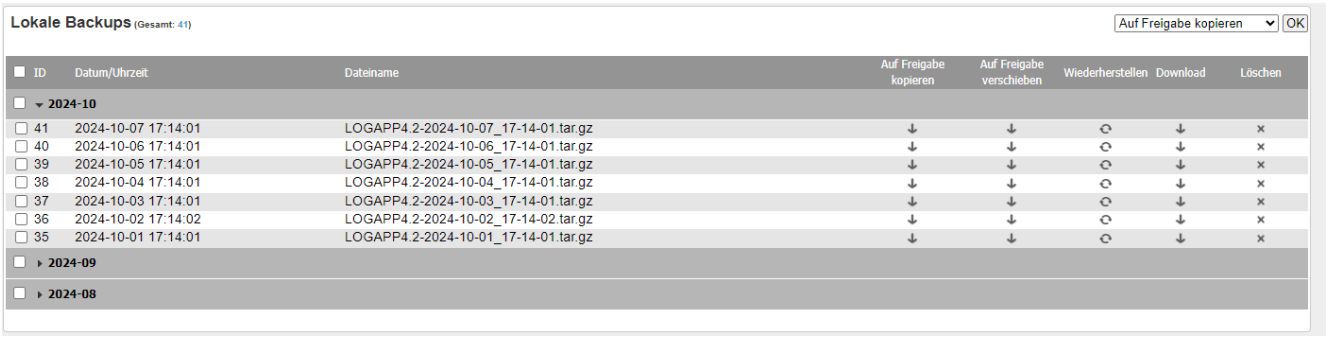

Abbildung 71: Lokale Backups

Es kann für die Backups auch ein SMB/CIFS-Freigabe, ein S3 Bucket (AWS), ein Azure Blob oder ein SSHFS angegeben werden.

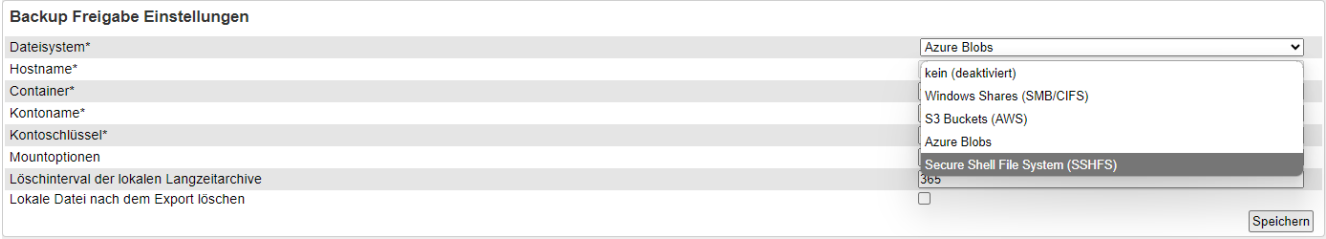

Abbildung 72: Backup Freigabe Einstellungen

Option	Beschreibung
Backup Freigabe Einstellungen	
Dateisystem	Auswahl des Dateisystems für das Langzeitarchiv, entweder SMB/CIFS-Freigabe oder lokal
Hostname	FQDN (Fully Qualified Domain Name) oder IP des File Servers
Freigabe	Freigabename auf dem File Server
Benutzername	Benutzername für die Authentifizierung
Passwort	Passwort für die Authentifizierung
Datenspeicher (S3 AWS)	Der S3 Bucket, in dem die Daten für das Langzeitarchiv gespeichert werden.
Zugriffsschlüssel-ID (S3 AWS)	AccessKeyId für den S3 Bucket (AWS). Sie wird verwendet, um auf die AWS-Ressourcen zuzugreifen und die Authentifizierung bei der Nutzung von AWS-Diensten sicherzustellen.
Geheimer Zugriffsschlüssel (S3 AWS)	SecretAccessKey für den S3 Bucket (AWS). Dieser Schlüssel wird zusammen mit der Zugriffsschlüssel-ID verwendet, um die Authentifizierung und den Zugriff auf AWS-Dienste zu gewährleisten.
Container (Azure)	Der Container bezieht sich auf die Azure Blob Storage. In Azure Storage ist ein Container eine logische Gruppierung von Blobs, die verwendet wird, um Daten zu organisieren und zu verwalten. Jeder Container kann mehrere Blobs enthalten, und der Container-Name muss innerhalb des Azure Storage-Kontos eindeutig sein.
Kontoname (Azure)	Der Kontoname bezieht sich auf den Namen des Azure Storage-Kontos. Jedes Azure Storage-Konto hat einen eindeutigen Namen, der im Azure-Portal verwendet wird, um auf die Ressourcen des Kontos zuzugreifen. Der Kontoname muss global eindeutig sein und wird verwendet, um auf die Blob-Daten zuzugreifen und diese zu verwalten.
Kontoschlüssel (Azure)	Der Kontoschlüssel ist ein geheim gehaltenes Passwort, das mit dem Azure Storage-Konto verknüpft ist.
Mountoptionen	Optionen, welche dem Linux Mount Befehl mitgegeben werden können, z.B. sec=ntlmv2i, DOMAIN='example, vers=2.0'. Details entnehmen Sie dazu den mount man pages. Zum Testen kann folgender Mount-Befehl verwendet werden (mit oben genannten Optionen): `sudo USER='YYY' PASSWD='XXX' mount -o sec=ntlmv2i,DOMAIN='ZZZ',uid=www-data,gid=www-data -t cifs //192.168.205.131/laa/ /archive/2/ 2>&1`
Lokale Datei nach dem Export löschen	Aktivieren, um das Archiv nur auf dem externen Share abzulegen (empfohlen)

Tabelle 15: Backup Freigabe Einstellungen

6.3 Benutzerverwaltung

Siehe Kapitel 4 - Allgemeine Einstellungen.

6.4 Log Quellen

Unter Log Quellen können alle verfügbaren Quellen von Logs eingebunden werden.

6.4.1 LogAgent

Installationsvoraussetzungen

Für die Installation eines Windows LogAgents muss auf dem Zielsystem eine Microsoft Visual C++ Redistributable 2015 oder höher installiert sein. Die Visual C++ Redistributables 2015 und 2017 werden mit dem LogAgent ausgeliefert. Der Windows Agent unterstützt die Betriebssysteme Windows Server 2012 / 2012 R2 oder höher

Der Linux Agent benötigt auf dem Zielsystem boost und openssl.

Folgende Linux Betriebssysteme werden unterstützt:

- Red Hat Enterprise Linux und CentOS ab Version 7
- Ubuntu ab Version 16.04
- Debian 8

Übersicht

Im Menü unter „LogAgent“ können LogAgents verwaltet werden. Bestehende LogAgents werden gruppiert nach Gerätegruppen in der Listenansicht angezeigt.

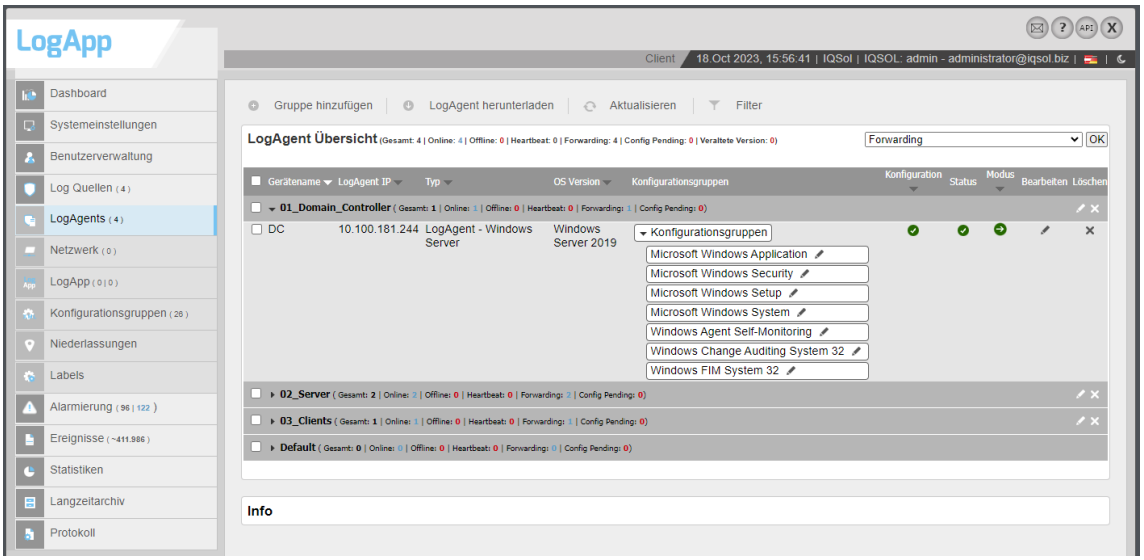

Abbildung 73: Übersicht LogAgent

Folgende Informationen werden in der Listenansicht angezeigt:

Option	Beschreibung
Gerätename	Name des LogAgents, (Hostname bei Windows und Linux Betriebssystemen)
LogAgent IP	IP-Adresse des LogAgents
Typ	Typ des LogAgents (Windows, Linux)
OS Version	Version des Betriebssystems
Konfigurationsgruppen	Zeigt alle zugewiesenen Konfigurationsgruppen. Standardmäßig sind diese ausgeblendet und lassen sich mit einem Klick auf „Konfigurationsgruppen“ aufklappen.
Konfiguration	Status der Agent-Konfiguration. Grünes Symbol, wenn der Agent eine aktuelle Konfiguration hat, blaues Symbol, wenn eine Konfiguration geändert wurde und noch freigegeben werden muss (und damit an den Agenten übertragen wird), violettes Dreiecksymbol, wenn die Konfiguration geändert und freigegeben wurde und noch nicht vom Agent abgeholt wurde.
Status	Status des LogAgents. Grünes Symbol, wenn regelmäßig Heartbeat-Nachrichten gesendet werden, graues Symbol, wenn der LogAgent keine Heartbeat Nachrichten sendet. Ein graues Warndreieck wird angezeigt, wenn die Version des Agents nicht aktuell ist und der Agent offline ist. Sollte der Agent online sein und veraltet so wird ein violettes Warndreieck angezeigt.
Modus	Betriebsmodus des LogAgents, kann durch Klicken umgeschaltet werden. Im Forwarding Modus (grünes Symbol) werden entsprechend der zugewiesenen Konfigurationsgruppen Ereignisse vom Agent gesendet, im Heartbeat Modus (gelbes Symbol) werden vom Agent nur Heartbeat-Nachrichten, aber keine Ereignisse gesendet.
Bearbeiten	Button für das Bearbeiten-Menü
Löschen	Button für eine Deinstallation des LogAgent

Tabelle 16: LogAgent Listenansicht

Mit einem Klick auf „Status“ öffnet sich eine genaue Übersicht über den LogAgent. Im ersten Tab „Status“ werden Informationen über die Verbindung zum Receiver, zum Heartbeat und zum FileIntegrityServer angezeigt. Zusätzlich werden die letzten erhaltenen Ereignisse, der letzte erhaltene Heartbeat und der letzte durchgeführte Scan mit Datum und Uhrzeit angezeigt. Darunter befindet sich ein leeres Textfeld, mit einem Klick auf den Button „Verbindung testen (pingen)“ wird ein Ping zum Agent durchgeführt. Die Ergebnisse erscheinen danach im zuvor leeren Textfeld.

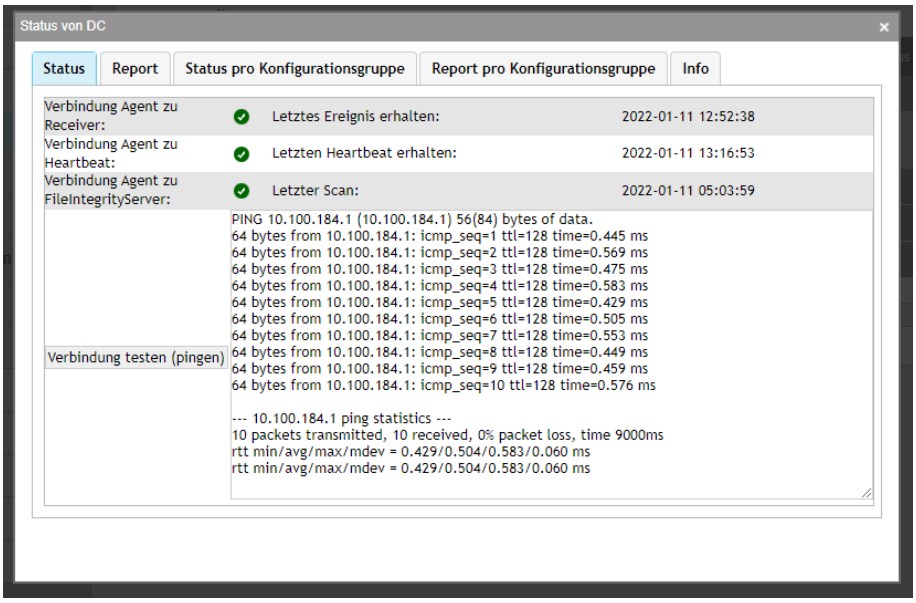

Abbildung 74: Status des LogAgent

Im zweiten Tab „Report“ werden Grafiken angezeigt. Es sind fünf unterschiedliche Grafiken verfügbar, welche verschiedene Zeiträume anzeigen.

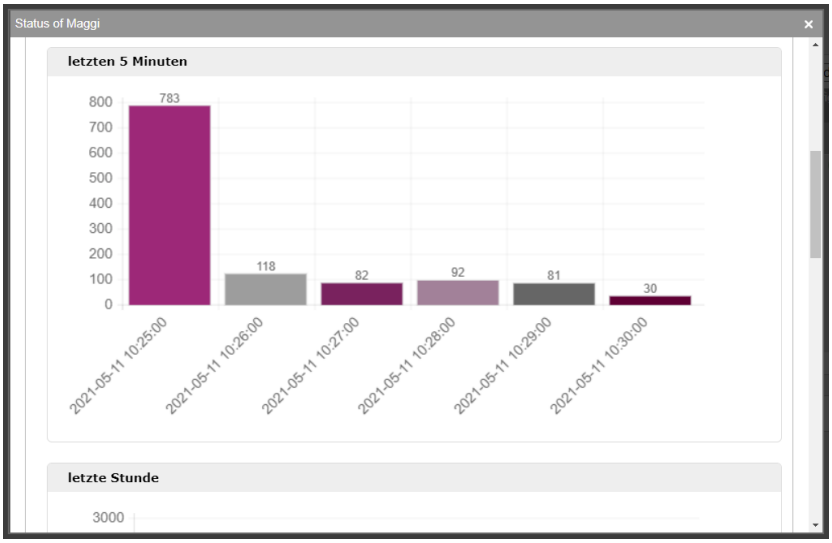

Abbildung 75: LogAgent Grafik

Der Tab „Status pro Konfigurationsgruppe“ enthält eine Auflistung der Konfigurationsgruppen und den Zeitpunkt, wann das letzte Ereignis von dieser Konfigurationsgruppe auf diesem Agenten empfangen wurde.

Der Tab „Report pro Konfigurationsgruppe“ ermöglicht es, ähnlich wie der Tab „Report“ Diagramme anzuzeigen, welche die Anzahl der Ereignisse für eine Konfigurationsgruppe in bestimmten Zeiträumen wiederzugeben.

Im Tab „Info“ sind kurze Informationen zum Tab „Status“ enthalten.

Um die angezeigten LogAgents in der Übersicht einzuschränken, stehen Filterfunktionen zur Verfügung, die eine Suche nach Name, IP-Adresse oder Typ ermöglichen.

Es wird empfohlen, LogAgents in Gerätegruppen zu organisieren. Gerätegruppen können mit dem Button „Gruppe hinzufügen“ angelegt werden.

Installation

Mit Hilfe des Buttons „LogAgent herunterladen“ können Installer für Windows und Linux sowie die für die manuelle Installation notwendigen Default-Zertifikate (nur bei aktiver Verschlüsselung) heruntergeladen werden. Diese können manuell oder mit einer Softwareverteilungslösung installiert werden. Bei Verwendung einer Softwareverteilungslösung ist darauf zu achten, die Agenten leicht zeitversetzt zu installieren.

Es sind aus Kompatibilitätsgründen neben der aktuellen Version des Windows Agenten auch Versionen für ältere Versionen verfügbar.

Um den Windows Agent manuell zu installieren, führen Sie das LogAppAgent Setup-Paket auf dem gewünschten Zielsystem aus, der Install-Wizard führt Sie durch die Installation. Neben dem Akzeptieren der Lizenzbedingungen müssen die IP des gewählten Interfaces für die Serverinstallation der LogApp und der Mandantenname sowie das Default-Zertifikat angegeben werden.

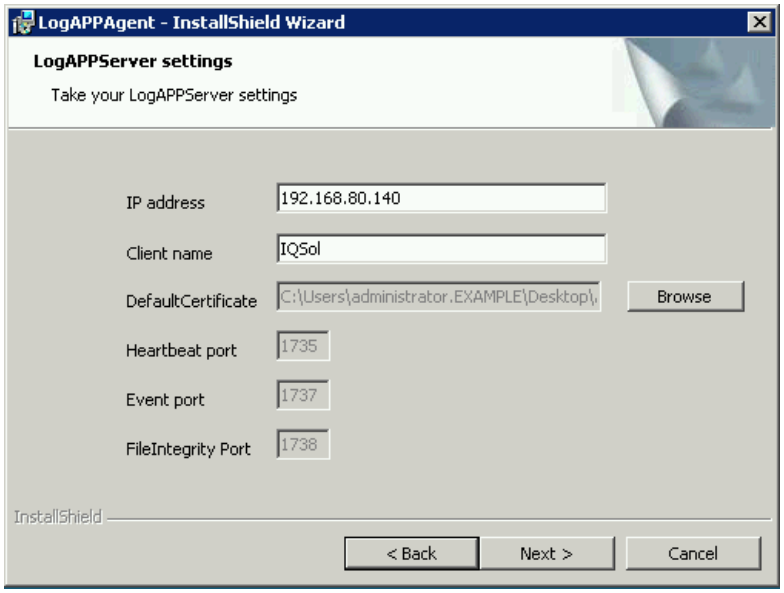

Abbildung 76: Manuelle Installation eines Windows LogAgents

Nach der Installation wird der Agent automatisch gestartet und verbindet sich zur LogApp.

Um den Linux Agent manuell zu installieren, entpacken Sie das tar.gz lokal auf dem Linux Server, auf welchem Sie den Agenten in Betrieb nehmen möchten. Anschließend führen Sie den Installer „LogAgentInstallerUI.sh“ aus. Während des Installationsprozesses werden das Installationszielverzeichniss, Mandantenname und die LogApp IP für das gewählte Interface für die Serverinstallation (ETH1, ETH0) abgefragt.

Weitere vorzunehmende Einstellungen sind:

Heartbeatport: Sollte der Port des Heartbeats auf der LogApp geändert worden sein, so muss hier der geänderte Port eingetragen werden.

Recieverport: Sollte der Port des Receivers auf der LogApp geändert worden sein, so muss hier der geänderte Port eingetragen werden.

User for LogAgent: Hier wird definiert, unter welchem User der LogAgent laufen soll. Sollte ein anderer Benutzer verwendet werden als der Standarduser (root), so ändern sich die Pfade des LogFiles, bzw der PID Files. Das LogAgentLogFile ist bei Standardkonfiguration unter /var/log zu finden, sollte der

LogAgent als nicht root Benutzer installiert sein, so befindet sich das Logfile unter /var/opt/logagent/. Außerdem sind die PIDFiles als nicht root Benutzer nicht unter /var/run zu finden, sondern auch unter /var/opt/logagent.

Die Wahl des Benutzers hat außerdem Folgen, welche LogFiles ausgelesen werden können und welche Verzeichnisse mit FIM überwacht werden können.

Encryption: hier kann festgelegt werden, ob der LogAgent verschlüsselte oder unverschlüsselte Verbindungen zur LogApp aufbauen soll

Path of default certificate: Hier ist das Verzeichniss anzugeben, in welchem sich das Defaultzertifikat befindet (AGENT_0.pem, welches im Installerarchiv enthalten ist).

```
root@iqsol-virtual-machine:~# ./LogAgentInstallerUI.sh
LogAgent Installer - User Interface
Installation Destination (default: /opt): /opt
LogApp IP address: 192.168.80.158
HeartBeat port (default: 1735): 1735
Receiver port (default: 1737): 1737
Client name: iqsol
User for LogAgent (default: root):
Encryption (default: true):
Path of default certificate (default: /tmp): /root
Installing LogAgent
Verifying archive integrity... All good.
Uncompressing LogAgent installer  100%
```

Abbildung 77: Manuelle Installation eines Linux Agents

Nach der Installation startet der Linux Agent automatisch und stellt eine Verbindung zur LogApp her.

Neu installierte LogAgents werden im Heartbeat-Modus betrieben. Bei einer Installation über die LogApp wird neuen LogAgents die Windows bzw. Linux Agent Self-Monitoring Konfigurationsgruppe zugewiesen, manuell installierten LogAgents werden keine Konfigurationsgruppen zugewiesen.

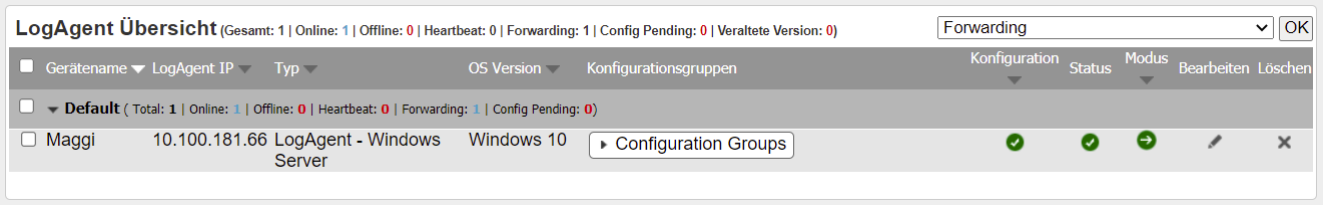

Abbildung 78: LogAgent in der Standardkonfiguration

NAT bei manueller Installation

Sollte NAT gewünscht sein, so ist dies bei der manuellen Installation durch die Angabe der NAT Adresse zu realisieren. Die LogApp erkennt automatisiert diese Abweichung und trifft die entsprechenden Einstellungen um NAT weiterhin zu verwenden.

Rollout mit Softwareverteilungslösungen

Für das Ausrollen von LogAgents mit Softwareverteilungslösungen sind folgende Aufrufe des Installationspaketes notwendig:

1. Windows

```
C:\LogAgentInstaller.exe /s /v"LOGAPPSERVERIP=[LogAppIP] LOGAPPSERVERNAME=logapp
LOGAPPSUBJECTNAME=AGENT_0 LOGAPPSERVERHBPORT=1735 LOGAPPSERVEREVTPORT=1737
LOGAPPAGENTID=0 LOGAPPCLIENTNAME=[ClientName] CHOOSENFILE=[CertPath] /qn"
```

Zum Beispiel:

```
C:\LogAgentInstaller.exe /s /v"LOGAPPSERVERIP=10.100.181.240
LOGAPPSERVERNAME=logapp LOGAPPSUBJECTNAME=AGENT_0 LOGAPPSERVERHBPORT=1735
LOGAPPSERVEREVTPORT=1737 LOGAPPAGENTID=0 LOGAPPCLIENTNAME=iqsol
CHOOSENFILE=C:\AGENT_0.p12 /qn"
```

Außerdem ist es möglich, mit dem /l Flag noch ein Logfile schreiben zu lassen.
Zum Beispiel:

```
C:\LogAgentInstaller.exe /s /v"LOGAPPSERVERIP=10.100.181.240
LOGAPPSERVERNAME=logapp LOGAPPSUBJECTNAME=AGENT_0 LOGAPPSERVERHBPORT=1735
LOGAPPSERVEREVTPORT=1737 LOGAPPAGENTID=0 LOGAPPCLIENTNAME=iqsol
CHOOSENFILE=C:\AGENT_0.p12 /le C:\InstallLog.txt /qn"
```

Mögliche Werte für dieses Flag sind:

i - Status messages
w - Nonfatal warnings
e - All error messages
a - Start up of actions
r - Action-specific records
u - User requests
c - Initial UI parameters
m - Out-of-memory or fatal exit information
o - Out-of-disk-space messages
p - Terminal properties
v - Verbose output
x - Extra debugging information
+ - Append to existing log file
! - Flush each line to the log
* - Log all information, except for v and x options

2. Linux

```
./LogAgentInstaller.sh --dest /opt --ip [LogAppIP] --hbPort 1735 --recPort 1737 --
client [ClientName] --user [Service user for LogAgent] --encryption true --cert
[Directory-path-to-certificate-but-without-the-actual-file]
```

Zum Beispiel:

```
./LogAgentInstaller.sh --dest /opt --ip 192.168.80.212 --hbPort 1735 --recPort
1737 --client iqsol --user root --encryption true --cert /tmp
```

Die Werte LogAppIP, ClientName und CertPath sind mit den Werten der konkreten Installation zu ersetzen. Auf Linux kann zusätzlich der ausführende Benutzer für den Agenten konfiguriert werden.

Wird der Installer über dieses Script ausgeführt, so gibt dieser einen Rückgabewert zurück, welcher unter anderem mit echo $? Ausgegeben werden kann.

Mögliche Rückgabewerte sind der folgenden Tabelle zu entnehmen:

Rückgabewert	Bedeutung
0	Erfolgreiche Installation
1	User der für den Installtionsvorgang verwendet wird ist kein root User

2	Ein notwendiger Parameter fehlt
3	Zielverzeichniss nicht gefunden
4	Installationspakete nicht gefunden
5	Vorrausgesetzte Pakete sind nicht installiert
6	Defaul Zertifikat nicht gefunden

Abbildung 79: Rückgabewerte Linuxagentinstaller

Installation von LogAgents auf Images

Soll der LogAgent auf einem Image installiert werden, welches von Lösungen wie Citirx verbreitet wird, ist es empfohlen eine andere Methode der Installation zu verwenden.

Als erstes sollte sichergestellt werden, dass bei der Erstellung keine Verbindung zur LogApp besteht. Der Grund ist, dass der Agent sich sonst bei der LogApp registriert nach erfolgreicher Installation.

Anschließend wird der LogAgent installiert und das Image erstellt. Sollte das Image nun ausgerollt werden und hierbei eine Verbindung zur LogApp aufgebaut werden, meldet sich der Agent bei Servicestart bei der LogApp und der Installationsvorgang wird abgeschlossen.

Für das Masterimage ist es empfohlen, den Dienst zu stoppen und ihn nicht automatisch starten zu lassen, da es sonst bei einer späteren Bearbeitung des Images vorkommen kann, dass sich der Agent bei der LogApp registriert und eine AgentID erhält. Dies würde dazu führen, dass alle ausgerollten Images mit der gleichen ID kommunizieren und es so den Eindruck erweckt, es gäbe es nur ein Device.

Häufige Fehler beim Installieren:

- Falsche IP /LogApp nicht erreichbar:
  Hat man eine falsche IP beim installieren eingegeben oder ist die LogApp generell nicht erreichbar, so wird im Agentlogfile eine Meldung ausgegeben, dass der Handshake nicht funktioniert hat (IOSERVICE (1735): Handshake failed).
  In den Details ist unter anderem zu sehen, dass das Socket nicht connected ist (“A request to send or receive data was disallowed because the socket is not connected”).

- Falscher Mandant:
  Wird ein nicht existierender Mandant angegeben, so befindet sich die Meldung „IOSERVICE (1735) - Communication error reading“ (Detail: short read) im Agent-Logfile.
  Auf der LogApp im superadmin-Bereich findet sich im AuditTrail unter Services die aussagekräftigere Meldung „Error Installing Agent (10.100.181.22). Client „iqsol“ is no valid client“

- Keine/nicht genügend Agentlizenzen:
  Wird der Agent installiert und es sind nicht mehr genügend Lizenzen vorhanden, so logged der Agent die Meldung „No free agent license“ ins Logfile und beendet sich anschließend.

LogAgent bearbeiten

Bestehende LogAgents können mittels der Buttons in der Listenansicht bearbeitet werden.

Im „Bearbeiten“-Menü können Gerätegruppe, Niederlassung, Lizenzen und Konfigurationsgruppen bearbeitet werden.

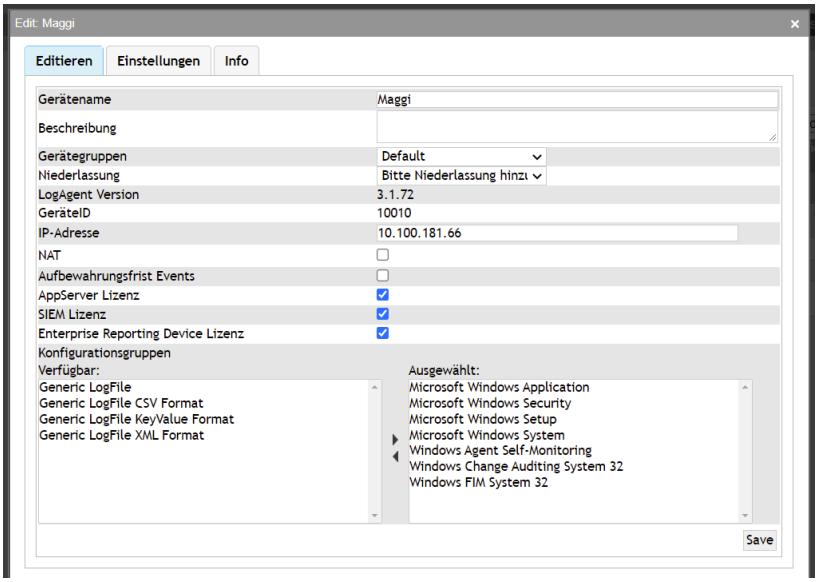

Abbildung 80: LogAgent bearbeiten

Folgende Optionen können bearbeitet werden:

Option	Beschreibung
Gerätename	Name des Gerätes
Beschreibung	Beschreibung des Gerätes
NAT	Wenn aktiviert, kann hier eine alternative Adresse definiert werden, welch statt der Adresse des SensorInterfaces verwendet wird. !!! ACHTUNG!!! Diese Adresse wird ab der nächsten Konfigurationsübertragung verwendet. Sollte NAT bei den betroffenen Geräten nicht eingerichtet sein, kann der Agent nicht mehr mit der LogApp kommunizieren.
Gerätegruppe	Zuordnung des LogAgents zu einer Gerätegruppe für die Gruppierung in der Listenansicht
Niederlassung	Zuordnung des LogAgents zu einer Niederlassung
Aufbewahrungsfrist Events	Hier kann eine Aufbewahrungsfrist in Tagen ausgewählt werden. Diese definiert, wie lange Ereignisse und Alarme, welche von diesem LogAgent empfangen wurden, aufbewahrt werden. Nach dieser Frist werden diese gelöscht.

LogAgent Version	Aktuelle Version des LogAgent (wird mit dem Heartbeat mitgesendet)
GeräteID	Interne ID des Gerätes
AppServer Lizenz	Zuweisung einer AppServer Lizenz. Dadurch kann dem LogAgent eine größere Auswahl an Konfigurationsgruppen zugewiesen werden.
Enterprise Reporting Device Lizenz	Zuweisung einer Enterprise Reporting Device Lizenz. Der Enterprise Reporting Server exportiert nur Ereignisse und Alarme von LogAgents und Syslog-Geräten mit einer solchen Lizenz.
Konfigurationsgruppen	Zuweisung von Konfigurationsgruppen an den LogAgent. Konfigurationsgruppen steuern, welche Ereignisse vom Agent an die LogApp gesendet werden.

Tabelle 17: LogAgent bearbeiten

Erweiterte Einstellungen

Im Tab Einstellungen können erweiterte Einstellungen zum Betrieb des LogAgents getroffen werden. Folgende Einstellungen stehen zu Verfügung:

DebugLevel

Bestimmt wie hoch das LogLevel des betroffenen LogAgents ist. Drei verschiedene Optionen stehen zur Verfügung.

- Aus: Es werden nur wichtige Systemereignisse protokolliert.
- Medium: externe Ergeinisse werden verstärkt protokolliert (Kommunikationsaufbau, LogfileRotationen, etc)
- Hoch: zusätzlich zu den anderen Ereignissen werden auch interne Informationen protokoliert, welche im Fehlerfall eine genaue Analyse ermöglichen. Dieser Level ist jedoch nur in Verbindung mit dem Support anzuraten, da dieser Level ein erhöhtes Logaufkommen verursacht.

XML Konfiguration

Diese Einstellungen regeln, wie sich der Agent im Betrieb verhält. Änderungen an diesen Einstellungen sind nur gemeinsam mit dem Support anzuraten. Da geänderte Einstellungen hier das Verhalten des Agenten unter Umständen stark beeinflussen können (Erhöhter CPU Verbrauch, etc.).

Mögliche Einstellungen:

Einstellung	Beschreibung
Forwarder->eventcount	Maximale Anzahl der Events, welche in einem Paket gesendet werden.
Forwarder->forwardtimer	Anzahl der Millisekunden, welche zwischen den Sendevorgängen eines Eventpaketes gewartet wird.
Forwarder->eventstorm	Diese Sektion behandelt, wie mit Eventstorms umgegangen wird. Ein Eventstorm ist eine große Anzahl an gleichen Events, welche innerhalb eines definierten Zeitraums auftreten. Tritt dies auf, so wird die Übertragung gedrosselt.
Forwarder->eventstorm->limit	Definiert die Anzahl an gleichen Events, welche als Eventstorm wahrgenommen werden.

	Ist dieses Setting 0 so kann es zu keinem Eventstorm kommen.
Forwarder->eventstorm->duration	Zeit in Millisekunden, welche als Beobachtungszeitraum für den Eventstorm dient.
Heartbeat->heartbeattimer	Anzahl der Millisekunden, welche zwischen zwei Sendevorgängen der Heartbeats gewartet wird

Tabelle 18: Xml Konfiguration LogAgent

6.4.2 Netzwerk

Im Untermenü Netzwerk werden der lokale Netzwerk-Proxy sowie Netzwerk-Proxys auf Agenten verwaltet.

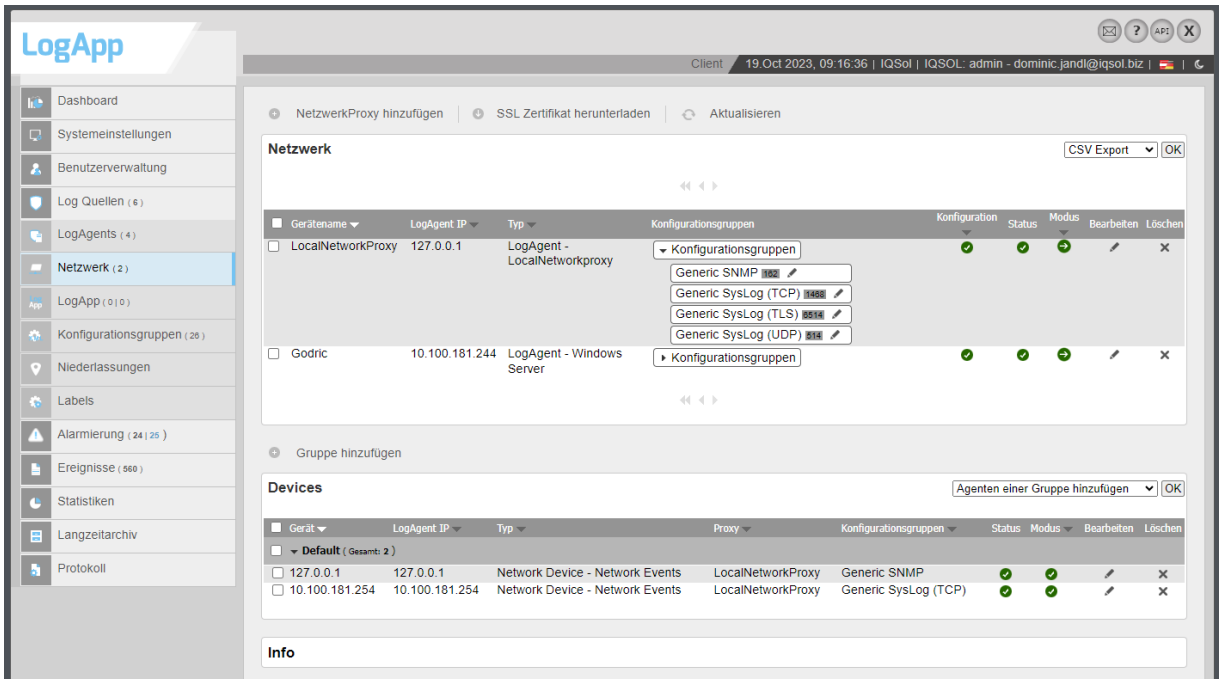

Abbildung 81: Netzwerk

In der Liste Netzwerk werden alle konfigurierten Netzwerk-Proxys angezeigt. Folgende Informationen werden angezeigt bzw. können folgende Aktionen durchgeführt werden.

Option	Beschreibung
Gerätename	Name des Agenten, welcher als Syslog-Proxy konfiguriert wurde oder der lokale Syslog-Proxy
LogAgent IP	IP Adresse des Agenten
Typ	Typ des Proxies (LogAgent –Windows, LogAgent –Linux, LogAgent – LocalNetworkProxy)
Konfigurationsgruppen	Die dem Syslog-Proxy zugewiesenen Syslog Konfigurationsgruppen.
Konfiguration	Status der Agent-Konfiguration. Grünes Symbol, wenn der Agent eine aktuelle Konfiguration hat, blaues Symbol, wenn eine Konfiguration geändert wurde und noch freigegeben werden muss (und damit an den Agenten übertragen wird), violettes Dreiecksymbol, wenn die Konfiguration geändert und freigegeben wurde und noch nicht vom Agent abgeholt wurde.

Status	Status des LogAgents. Grünes Symbol, wenn regelmäßig Heartbeat-Nachrichten gesendet werden, rotes Symbol, wenn der Agent keine Heartbeat Nachrichten sendet.
Modus	Betriebsmodus des LogAgents, kann durch Klicken umgeschaltet werden. Im Forwarding Modus (grünes Symbol) werden entsprechend der zugewiesenen Konfigurationsgruppen Ereignisse vom Agent gesendet, im Heartbeat Modus (gelbes Symbol) werden vom Agent nur Heartbeat-Nachrichten, aber keine Ereignisse gesendet.
Bearbeiten	Button für das Bearbeiten-Menü
Löschen	Button für die Entfernung des LogAgents als Netzwerkproxy.

Tabelle 19: Netzwerk-Proxy Listenansicht

In der Liste Devices werden alle Geräte angezeigt, welche an einen Netzwerkproxy Syslog-Nachrichten senden. Diese können zur besseren Übersicht gruppiert werden (Button Gruppe hinzufügen).

Mit dem Button „NetzwerkProxy hinzufügen“ können der lokale NetzwerkProxy („logapp“) oder ein anderer installierter LogAgent als NetzwerkProxy konfiguriert werden. Der NetzwerkProxy wird in der Liste Netzwerk angezeigt.

6.4.3 LogApps

In dieser Ansicht befinden sich LogApps welche auf dieses System Ereignisse weiterleiten.

Diese LogApps müssen am Quell-System konfiguriert werden und melden sich anschließend auf dem Zielsystem. Das zur Aktivierung benötigte Standard-Zertifikat kann über die Schaltfläche „Zertifikat herunterladen“ heruntergeladen werden. Dieses Archiv muss beim Aktivieren auf der Quell-LogApp verwendet werden.

Die Zahlen im Menü geben hier an wieviele LogApps an das Zielsystem senden (erste Zahl) und wieviele LogAgents über diese LogApps Ereignisse an die Ziel-LogApp weiterleiten (zweite Zahl).

LogApp bearbeiten

Bestehende LogApps können mittels der Buttons in der Listenansicht bearbeitet werden.

Es können die gleichen erweiterten Einstellungen (Kapitel Erweiterte Einstellungen), wie bei LogAgents bearbeitet werden.

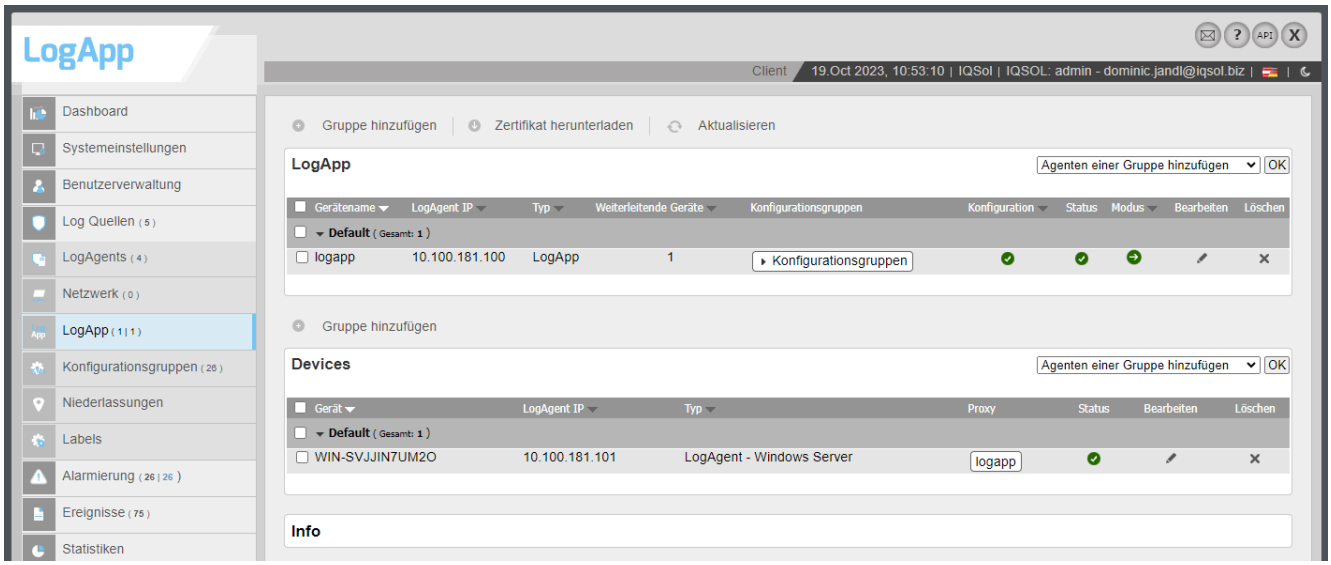

Abbildung 82: Übersicht Log Quellen LogApp

6.4.4 Konfigurationsgruppen

Konfigurationsgruppen steuern, welche Ereignisse aus welchen Quellen von den LogAgents gesendet werden. Die unterschiedlichen Konfigurationsgruppentypen werden nachfolgend im Detail erklärt.

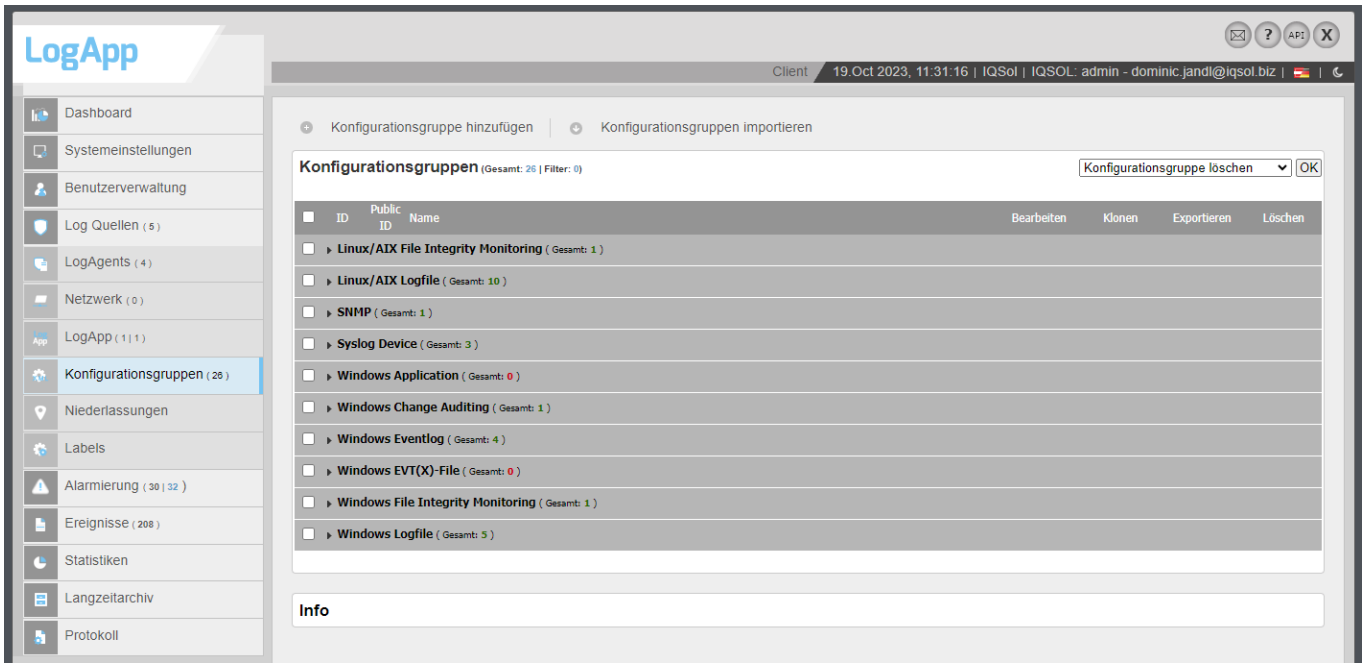

Abbildung 83: Konfigurationsgruppen

Um eine neue Konfigurationsgruppe anzulegen, klicken Sie den Button „Konfigurationsgruppe hinzufügen“. Konfigurationsgruppen müssen einem LogAgent zugewiesen werden, um aktiv zu werden.

Importieren von Konfigurationsgruppen

Mit der Schaltfläche „Konfigurationsgruppen importieren“ lassen sich Konfigurationsgruppen, welche vorher bereits exportiert wurden wieder importieren.

Nach einem Klick auf diese Schaltfläche wird man aufgefordert ein tar.gz Archiv auszuwählen welches hochgeladen wird.

Im darauf erscheinenden Fenster werden die Konfigurationsgruppen gelistet, welche im Export enthalten sind.

In diesem Fenster werden Name und Typ der Konfigurationsgruppe aufgelistet, ebenso wird angegeben ob sich auf der LogApp bereits eine Konfigurationsgruppe mit gleichem Namen und Typ befindet.

Um der LogApp mitzuteilen, was mit den Konfigurationsgruppen geschehen soll gilt es eine oder keine Aktion zu setzen (Checkboxen für Konfigurationsgruppen importieren/updaten).

Existiert die Konfigurationsgruppe noch nicht, so kann entschieden werden, ob die Konfigurationsgruppe importiert wird oder nicht.

Sollte die Konfigurationsgruppe bereits existieren kann entschieden werden ob die bereits existierende Gruppe aktualisiert wird, oder ob eine neue Gruppe hinzugefügt wird. Diese neue Gruppe erhält dann ein Suffix „_import“.

Der Vorgang wird mit einem Klick auf Speichern abgeschlossen.

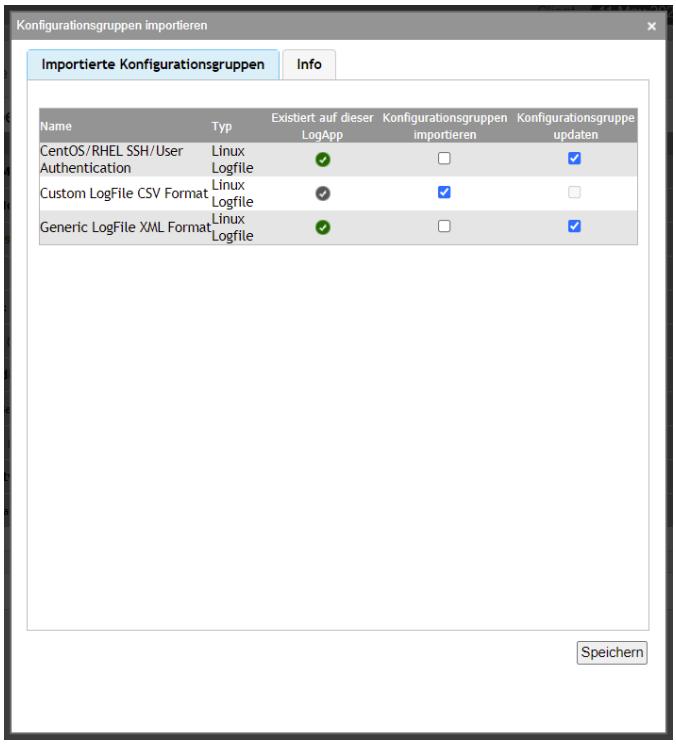

Abbildung 84 Import von Konfigurationsgruppen

Bulkoperations

Neben den Aktionen, welche bei jeder einzelnen Konfigurationsgruppe ausgeführt werden können (Editieren, Klonen, exportieren und löschen) können die Aktionen „Konfigurationsgruppe löschen“ und „Konfigurationsgruppe exportieren“ auch über eine BulkAction ausgelöst werden.

Hierzu markieren sie einfach die entsprechenden Konfigurationsgruppen mit den Checkboxen in der Tabelle, wählen eine Aktion im Dropdown Menü rechts oben aus und bestätigen mit einem Klick auf OK rechts neben dem Dropdown.

Konfigurationsgruppentypen

Linux LogFile / Windows LogFile

Linux Flatfile Konfigurationsgruppen werden verwendet, um Ereignisse aus textbasierten Logdateien auszulesen. Folgende Angaben müssen gemacht werden:

Option	Beschreibung
Basiseinstellungen	
Name	Name der Konfigurationsgruppe
Public ID	Diese ID wird verwendet, sollten Events von dieser Konfigurationsgruppe an eine LogApp wietergeleitet werden. Die Public ID muss am Ziel und am Quellsystem identisch sein, um eine reibungslose Funktion sicherzustellen.
Aufbewahrungsfrist Events	Eine Aufbewahrungsfrist in Tagen kann ausgewählt werden. Diese definiert, wie lange Ereignisse und Alarme, welche über diese Gruppe empfangen wurden, aufbewahrt werden. Nach dieser Frist werden sie gelöscht.
Pfad	Pfad zur Logdatei, Pfade können mit Wildcards angegeben werden, z.B.: c:\windows\log.txt c:\windows\log.* /var/log/logfile.txt /var/log/*.log /var/log/logfile.* Bei verwendeter Wildcard wird immer jene Datei gelesen, die dem Wildcard-Schema entspricht und als letztes geändert wurde.
File DiscoveryMode	Folgende Modi sind verfügbar: • Rotation Mode: Im Rotation Mode wird jedes File, welches auf den Pfadnamen matcht zur Überprüfung hergezogen. • New File Mode: Beim New File Mode werden nur Files zur Überprüfung herangezogen, welche auf den Pfadnamen matchen und ein Erstellungsdatum haben welches neuer oder gleich alt wie das zuletzt überprüfte File ist.
Modus	Folgende Modi sind verfügbar: • Webserver Format style • Key/Value • XML • CSV Die Funktionsweise der einzelnen Modi können im Anhang (Konfiguration für Logfiles und Syslog) nachgeschlagen werden.

Mehrzeilenmodus	Hier kann angegeben werden ob ein zu parsender Logeintrag mehrere Zeilen umfasst. Hierbei gibt es vier verschiedene Auswahlmöglichkeiten: • Deaktiviert: Logeinträge sind einzeilig • Anhand von Zeilen: hier kann eine fixe Anzahl von Zeilen definiert werden, welche zu einem Logeintrag zusammengefügt werden. Wenn ein Identifier matched werden ab dieser Zeile die hier angegebene Anzahl (minus eins) an Zeilen zu der ursprünglichen Nachricht hinzugefügt, so dass das Event die angegebene Anzahl an Zeilen enthält. • Ereignis endet mit Regex: in diesem Modus kann eine RegEx angegeben werden, welche das Ende eines Logeintrages definiert. • Nächstes Ereignis startet mit Regex: Mithilfe dieses Modus und der definierten RegEx wird bestimmt wann das nächste Ereignis startet. Alles vorangegangene Neue wird zu einem Logeintrag zusammengefasst. Sollte das Logfile zu Ende gelesen werden, so wird dies wie der Anfang eines neuen Logeintrags gehandhabt. Wird der Mehrzeilenmodus verwendet so werden für die Verarbeitung alle Zeilenumbrüche entfernt. Somit sind sie nicht in der Parsemap zu berücksichtigen.
Zeitformat	Format der Zeitangaben in der Logdatei, z.B. dd/MM/yyyy:HH:mm:ss
CultureInfo	Spracheneinstellung zur Interpretation von Monatsangaben in Zeitstempel (z.B. Jan (en) vs. Jän (de))
XML Konfiguration	Mit Klick auf die Schaltfläche öffnet sich der Parsemapeditor. Details zum Aufbau der XML Konfiguration finden Sie im Anhang (Konfiguration für Logfiles und Syslog).

Tabelle 20: Flatfile Konfigurationsgruppe

!!! Achtung !!! Es wird empfohlen, keine Files über 20 MB einzulesen, da dies zu einem erhöhten CPU-Verbrauch und /oder Verzögerungen bei der Eventübertragung führen kann.

Rotation

Die meisten Betriebssysteme unterstützen eine Art der Logfilerotation. Wird ein Logfile rotiert so versucht der Agent, das rotierte File ausfinding zu machen (z.B. /var/log/logfile.1) und eventuell vor der Rotation noch nicht übertragene Events auszulesen.

Folgende Kompressionstypen werden unterstützt:

- **Keine Komprimierung**: rotierte Files werden als Textfile weitergeführt
- **Tar Komprimierung (tarballs):** .tar
- **Gzip Komprimierung:** Dateinamenerweiterung .gz oder .tar.gz
- **LZW Komprimierung:** Dateinamenerweiterung .Z

Syslog Device

Durch die Zuweisung von Syslog Konfigurationsgruppen funktioniert der LogAgent als Syslog Proxy für Geräte, die Syslog Nachrichten senden (typischerweise Netzwerkgeräte wie Switches oder Firewalls). Wird eine Syslog Gruppe zugewiesen, startet der LogAgent einen Syslog-Listener auf dem konfigurierten Port, um Nachrichten entgegenzunehmen. Das System, dessen Nachrichten verarbeitet werden sollen, muss konfiguriert werden, Syslog Nachrichten an die IP-Adresse und den konfigurierten Port des LogAgents zu senden.

Für jeden LogAgent kann pro Port eine Konfigurationsgruppe hinterlegt werden. An diesen Port können verschiedene Geräte des gleichen Typs Syslog Nachrichten senden. Wenn ein Agent als Syslog Proxy für verschiedene Gerätetypen eingesetzt werden soll, müssen dafür unterschiedliche Ports verwendet werden.

Folgende Angaben müssen gemacht werden:

Option	Beschreibung
Name	Name der Konfigurationsgruppe
Public ID	Diese ID wird verwendet, sollten Events von dieser Konfigurationsgruppe an eine LogApp wietergeleitet werden. Die Public ID muss am Ziel und am Quellsystem identisch sein, um eine reibungslose Funktion sicherzustellen.
Aufbewahrungsfrist Events	Eine Aufbewahrungsfrist in Tagen kann ausgewählt werden. Diese definiert, wie lange Ereignisse und Alarme, welche über diese Gruppe empfangen wurden, aufbewahrt werden. Nach dieser Frist werden sie gelöscht.
Protokoll	Hier kann das zur Übertragung gewünschte Protokoll spezifiziert werden. Zur Auswahl stehen: • UDP • TCP
Port	Hier wird der Port für den Listener definiert. Dieser Port darf nicht von anderen Konfigurationsgruppen oder anderen Applikationen belegt sein
Verschlüsselung	Wird als Protokoll TCP gewählt gibt es die Möglichkeit einer Verschlüsselung. Für Details zur Konfiguration sehen sie bitte den Anhang „Konfiguration für Syslog Over SSL“ ein
Webserver Format Style	Hier wird der Parse Modus festgelegt. Sollte Webserver Format Style aktiviert sein so wird Webserver Format Style angewendet, sonst Key/value.
Zeitformat	Format der Zeitangaben in der Logdatei, z.B. dd/MM/yyyy:HH:mm:ss
CultureInfo	Spracheneinstellung zur Interpretation von Monatsangaben in Zeitstempel (z.B. Jan (en) vs. Jän (de))
XML Konfiguration	Mit Klick auf die Schaltfläche öffnet sich der Parsemapeditor. Details zum Aufbau der XML Konfiguration finden Sie im Anhang (Konfiguration für Logfiles und Syslog).

SNMP

Ähnlich der Konfiguration für Syslog, können diese Konfigurationsgruppen einem Porxy zugewiesen werden. Der Proxy startet dann auf dem definierten Port einen SNMPv2 Trap Listener.

Folgende Angaben müssen gemacht werden:

Option	Beschreibung
Name	Name der Konfigurationsgruppe
Public ID	Diese ID wird verwendet, sollten Events von dieser Konfigurationsgruppe an eine LogApp wietergeleitet werden. Die Public ID muss am Ziel und am Quellsystem identisch sein, um eine reibungslose Funktion sicherzustellen.
Aufbewahrungsfrist Events	Eine Aufbewahrungsfrist in Tagen kann ausgewählt werden. Diese definiert, wie lange Ereignisse und Alarme, welche über diese Gruppe empfangen wurden, aufbewahrt werden. Nach dieser Frist werden sie gelöscht.
Port	Hier wird der Port für den Listener definiert. Dieser Port darf nicht von anderen Konfigurationsgruppen oder anderen Applikationen belegt sein
Webserver Format Style	Hier wird der Parse Modus festgelegt. Sollte Webserver Format Style aktiviert sein so wird Webserver Format Style angewendet, sonst Key/value.
Zeitformat	Format der Zeitangaben in der Logdatei, z.B. dd/MM/yyyy:HH:mm:ss
CultureInfo	Spracheneinstellung zur Interpretation von Monatsangaben in Zeitstempel (z.B. Jan (en) vs. Jän (de))
XML Konfiguration	Mit Klick auf die Schaltfläche öffnet sich der Parsemapeditor. Details zum Aufbau der XML Konfiguration finden Sie im Anhang (Konfiguration für Logfiles und Syslog).

Der Standard für SNMPv2 Traps sieht folgendes Format vor:

1 [Commuintystring] [RequestID] [Error-status] [Error-index] 1.3.6.1.2.1.1.3.0 [Timestamp] 1.3.6.1.6.3.1.1.4.1.0 [EnterpriseIDentifier] [VariablenOID1] [VariablenWert1]

Die Werte VariablenOID und VariablenWert können beliebig oft wiederholt werden.

Linux File Integrity Monitoring/Windows File Integrity Monitoring

Linux File Integrity Monitoring Konfigurationsgruppen ermöglichen zyklische Überprüfung der Integrität von Dateien auf Linux bzw. Windows Systemen. Durch die Erstellung von Prüfsummen in konfigurierbaren Intervallen kann der LogAgent Änderungen an Dateien seit der letzten Überprüfung feststellen. Für jede geänderte Datei wird ein Ereignis erzeugt.

Folgende Angaben müssen gemacht werden:

Option	Beschreibung
Name	Name der Konfigurationsgruppe
Public ID	Diese ID wird verwendet, sollten Events von dieser Konfigurationsgruppe an eine LogApp wietergeleitet werden. Die Public ID muss am Ziel und am Quellsystem identisch sein, um eine reibungslose Funktion sicherzustellen.
Aufbewahrungsfrist Events	Eine Aufbewahrungsfrist in Tagen kann ausgewählt werden. Diese definiert, wie lange Ereignisse und Alarme, welche über diese Gruppe empfangen wurden, aufbewahrt werden. Nach dieser Frist werden sie gelöscht.
Zeitpunkt	Zeitpunkt der Überprüfung
Wochentag	Wochentage, an denen die Überprüfung zu angegebenen Zeit ausgeführt wird
Rekursiv	Rekursive Prüfung mit Einbeziehung von Unterordnern
Pfad	Pfade, die überprüft werden, z.B. /etc.
Filter	Auswahl Black- oder Whitelist für Filterkriterien
Blacklist	Pfade oder Wildcard-Angaben, die bei der Prüfung ausgenommen werden, z.B. /etc/fonts. Diese Angaben können hierbei absolut oder relativ zu den Pfaden, welche unter Pfad angegeben werden, definiert werden. Für Details zum Unterschied zwischen Filefilter und Directoryfilter siehe Anhang „Black und Whitelist bei Fileintegritymonitoring“
Whitelist	Pfade oder Wildcard-Angaben, die bei der Prüfung exklusiv eingeschlossen werden, z.B. *.log. Diese Angaben können hierbei absolut oder relativ zu den Pfaden, welche unter Pfad angegeben werden, definiert werden. Für Details zum Unterschied zwischen Filefilter und Directoryfilter siehe Anhang „Black und Whitelist bei Fileintegritymonitoring“

Tabelle 21: Windows File Integrity Monitoring Konfigurationsgruppen

Bitte beachten Sie, dass File Integrity Überprüfungen, je nach Anzahl und Größe der zu überprüfenden Dateien, mehrere Stunden dauern können. Wenn einem Agenten mehrere Konfigurationsgruppen mit zu kurzen Zeiträumen zwischen den Ausführungsintervallen zugewiesen werden, werden vom Agent anstehende File Integrity Überprüfungen erst nach Abschluss der aktuell laufenden Überprüfung ausgeführt. File Integrity Überprüfungen werden nicht parallel, sondern immer hintereinander ausgeführt.

FileIntegrity liefert folgende Events:

- Neue/geänderte/gelöschte Files
- Neue/gelöschte Directories

Zusätzlich zu den Informationen, was mit welchem Ziel (File/Directory) geschehen ist, liefert das Ereignis auch den letzten Modifizierungszeitstempel. Dieser wird direkt vom betroffenen System ausgelesen und kann bei unter Umständen falscher Konfiguration (z.B. falsche Zeitzone am Ziel) vom tatsächlichen Modifizierungszeitstempel abweichen.

Windows Application

Windows Application Konfigurationsgruppen dienen der Einbindung von proprietären Logformaten von Drittprodukten auf Windows Systemen.

Windows Eventlog

Die Windows Eventlog Konfigurationsgruppen dienen dem Auslesen von lokalen Windows Eventlog-Einträgen durch den Agenten.

Folgende Angaben müssen gemacht werden:

Option	Beschreibung
Basiseinstellungen	
Name	Name der Konfigurationsgruppe
Public ID	Diese ID wird verwendet, sollten Events von dieser Konfigurationsgruppe an eine LogApp wietergeleitet werden. Die Public ID muss am Ziel und am Quellsystem identisch sein, um eine reibungslose Funktion sicherzustellen.
Aufbewahrungsfrist Events	Eine Aufbewahrungsfrist in Tagen kann ausgewählt werden. Diese definiert, wie lange Ereignisse und Alarme, welche über diese Gruppe empfangen wurden, aufbewahrt werden. Nach dieser Frist werden sie gelöscht.
Stufen	Auswahl verschiedener Prioritäten von Ereignissen aus Anwendungslogs, die vom LogAgent übertragen werden sollen. Die Windows Protokolle Sicherheit und System unterscheiden Einträge nicht nach Prioritäten, in diesen Fällen sind alle Einträge von der Priorität Information.
Log	Windows Eventlog, aus dem Events ausgelesen werden, z.B. Security oder Application Log oder benutzerdefinierte Logs (Channel) bei Event von installierter Software.

Log Quelle	
Log Quelle	Log Quelle bei Anwendungslogs (z.B. Winlogon oder MsiInstaller). Angaben können als Black- oder White-List gemacht werden. Wenn keine Einschränkungen getroffen werden, werden alle Events abgeholt.
Event IDs	
Event IDs	Event IDs als Black- oder White-List. Wenn keine Einschränkungen getroffen werden, werden alle Events abgeholt.
Parse Map	
XML Konfiguration	Mithilfe einer Parsemap können zusätzliche Informationen aus der Raw Message übernommen worden. Diese Parsemap hat Standardmäßig den Mode Key/Value.

Tabelle 22: Windows Eventlog Konfigurationsgruppen

Windows EVT(X)-File

Windows EVT(X)-File Konfigurationsgruppen ermöglichen das Auslesen von Ereignissen aus Windows Eventlog-Exporten im EVT oder EVTX Format.

Folgende Angaben müssen gemacht werden:

Option	Beschreibung
Name	Name der Konfigurationsgruppe
Public ID	Diese ID wird verwendet, sollten Events von dieser Konfigurationsgruppe an eine LogApp wietergeleitet werden. Die Public ID muss am Ziel und am Quellsystem identisch sein, um eine reibungslose Funktion sicherzustellen.
Aufbewahrungsfrist Events	Eine Aufbewahrungsfrist in Tagen kann ausgewählt werden. Diese definiert, wie lange Ereignisse und Alarme, welche über diese Gruppe empfangen wurden, aufbewahrt werden. Nach dieser Frist werden sie gelöscht.
Pfad	Pfad zur EVT/EVTX-Datei, Pfade können mit Wildcards angegeben werden, z.B.: C:\Logs\MyLog.evtx C:\Logs*.evt C:\Logs\MyLog.*

Tabelle 23: Windows EVT(X)-Konfigurationsgruppen

6.4.5 Niederlassungen

Niederlassungen dienen dazu, LogAgents einer geografischen Position, z.B. der Firmenzentrale oder einer Außenstelle, zuzuordnen.

Über den Button „Niederlassung hinzufügen“ können neue Niederlassungen eingetragen werden.

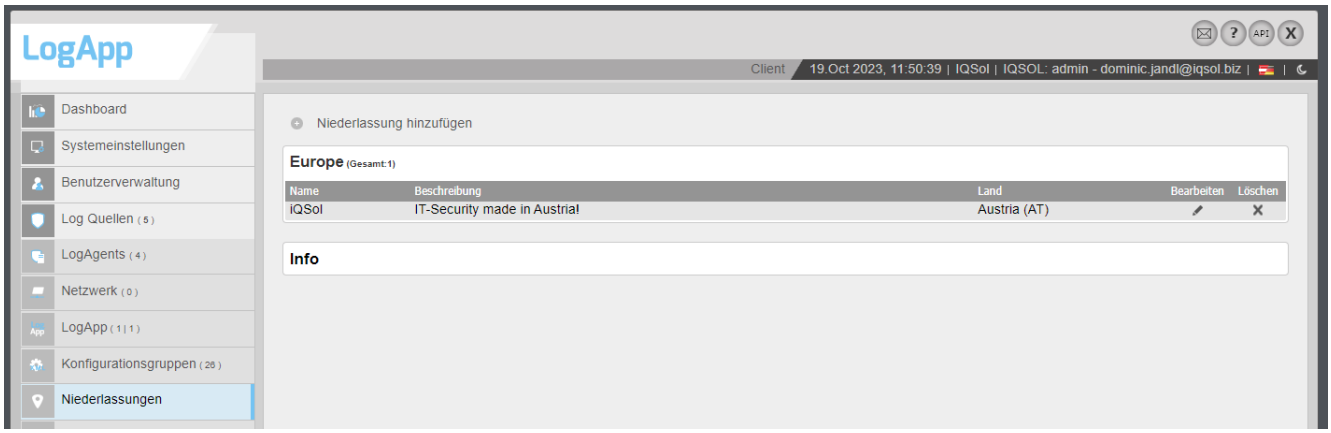

Abbildung 85: Niederlassungen

6.4.6 Labels

Werden in einer Parsemap ein oder mehrere generische Felder (evt_detail1-evt_detail30) verwendet, so können hier frei wählbare Namen für diese Spalten definiert werden.

Die Zuordnung welches Event welches Label verwenden soll, erfolgt durch Angabe der LabelmapID(<labelmapid>[ID des jeweiligen Labels]</labelmapid>) in einer XML Parsemap.

Details zum Aufbau der XML Konfiguration können im Anhang (Konfiguration für Logfiles und Syslog) nachgeschlagen werden.

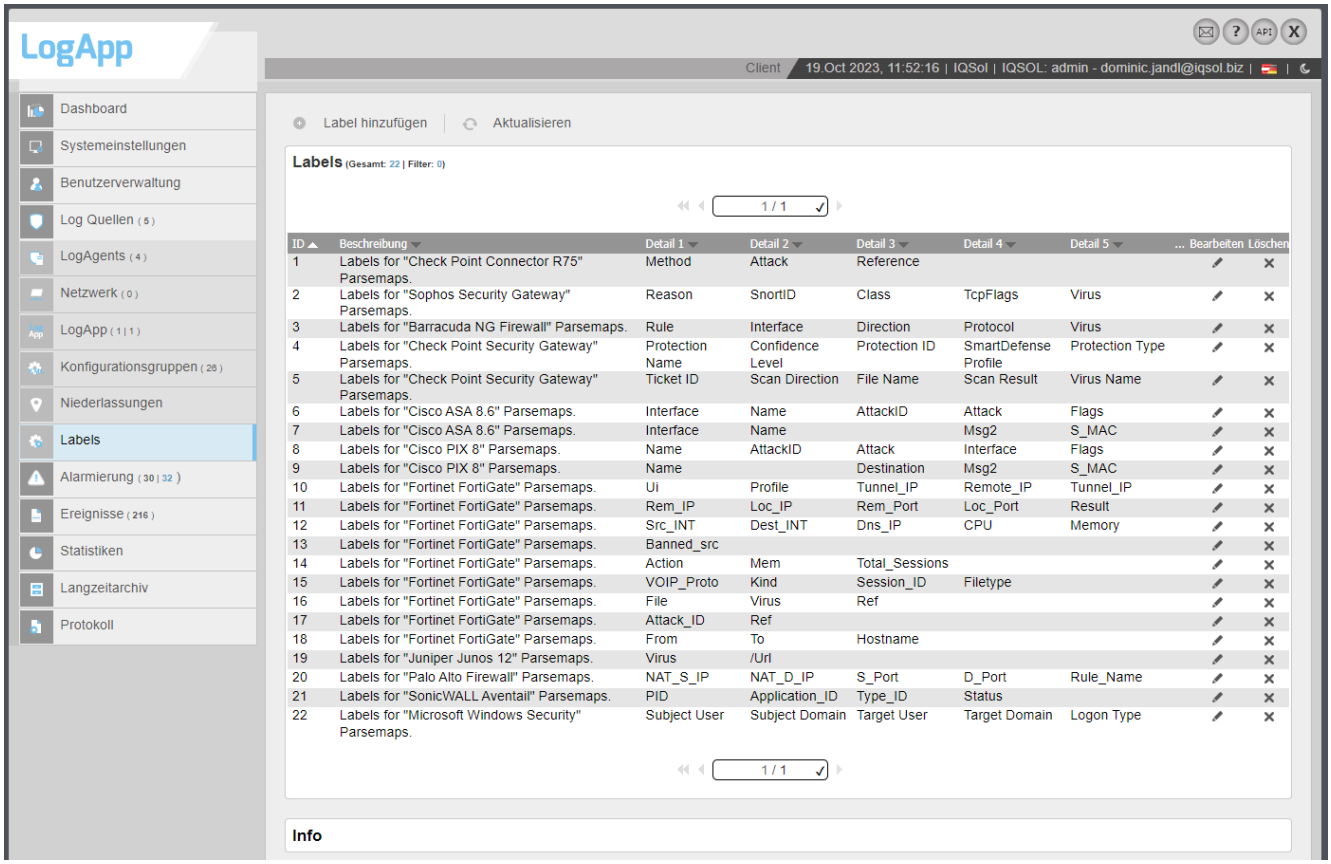

Abbildung 86: Labels

7 Alarme und Events

7.1 Alarmierung

Der Menüeintrag Alarmierung enthält zwei Zähler.

Der erste Zähler steht für die Anzahl der Alarme, welche (unabhängig vom Status) eine Priorität von niedrig bis hoch haben. Der zweite Zähler zeigt die Anzahl der Alarme an, welche den Status „Neu“ aufweisen:

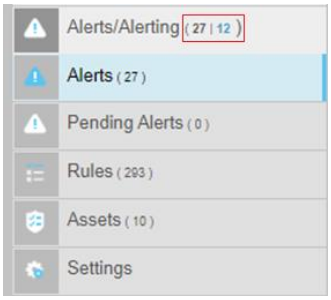

Abbildung 87: Menü Alarmierung

In diesem Beispiel gibt es somit 27 Alarme, von welchen sich 12 Alarme im Status „Neu“ befinden.

7.1.1 Alarme

Im Menüpunkt „Alarme“ werden die Alarme von den unterschiedlichen LogQuellen angezeigt. Alle eingehenden Ereignisse werden vom AlertParser Dienst gegen ein hinterlegtes Regelwerk (7.1.3 Regeln) geprüft. Wenn eine Übereinstimmung festgestellt wird, wird ein neuer Alarm generiert.

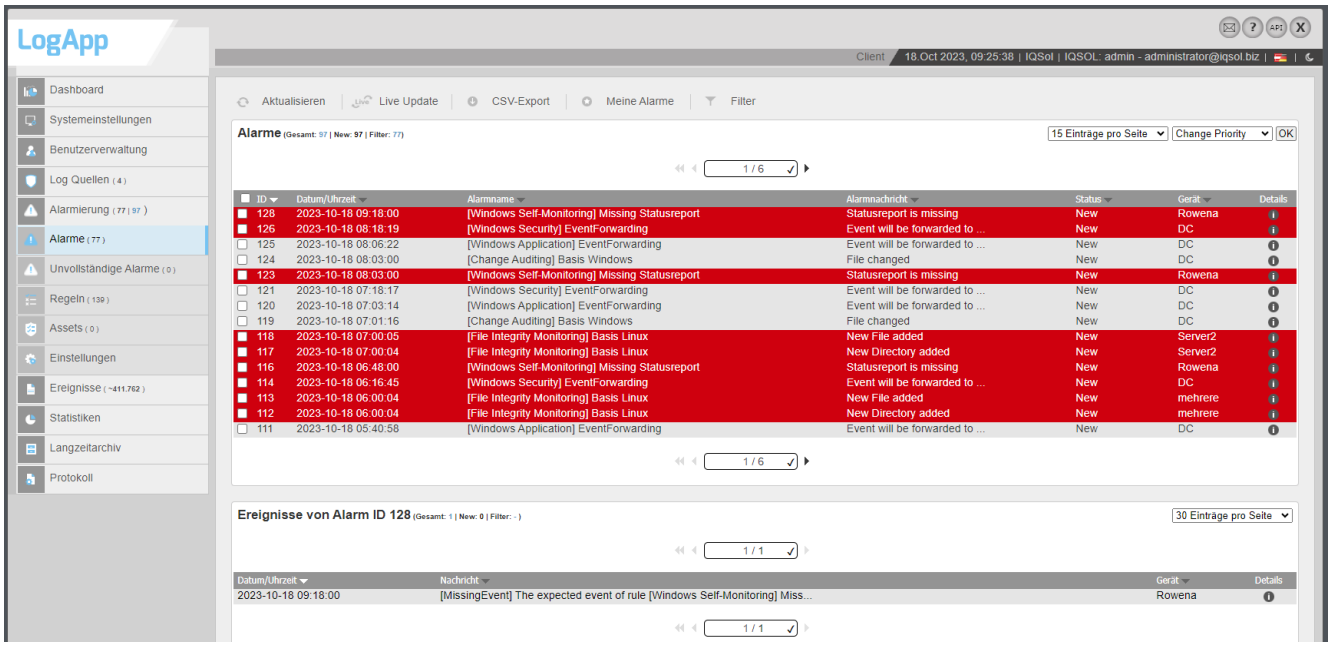

Abbildung 88: Alarme

Im oberen Bereich der Seite werden die Alarme in Tabellenform angezeigt. Die Alarme können mit den Buttons über der Tabelle aktualisiert, exportiert oder gefiltert werden.

Wird das „Live Update“ – Icon in Farbe angezeigt, so ist dies aktiviert und die Alarme werden in einem vorgegebenen Intervall stetig aktualisiert. Ist das Icon grau, so ist das Live Update deaktiviert.

Mit einem Klick auf den Button „Meine Alarme“ werden jene Alarme angezeigt, welche einem selbst zugewiesen sind/wurden.

Neben der Überschrift Alarme sind weitere Counter zu finden. Die ersten zwei sind analog zu den Countern im Menüeintrag Alarmierung und geben die Gesamtanzahl der Alarme (welche eine Priorität von Niedrig bis Hoch haben, unabhängig vom Status), sowie die Alarme mit Status Neu an.

Der dritte Counter bezieht sich auf einen eventuell angewandten Filter und gibt die Anzahl der Alarme zurück, welche auf diesen Filter zutreffen. Der Standardfilter, welcher beim Aufruf der Seite verwendet wird, liefert alle Alarme, welche einen Status besitzen der nicht Resolved ist und eine Priorität von Niedrig bis Hoch haben.

Abbildung 89: Alarm Counter

Durch einen Klick auf eine Zeile können Einträge selektiert werden. In der unteren Tabelle werden jeweils die Ereignisse angezeigt, die den ausgewählten Alarm verursacht haben.

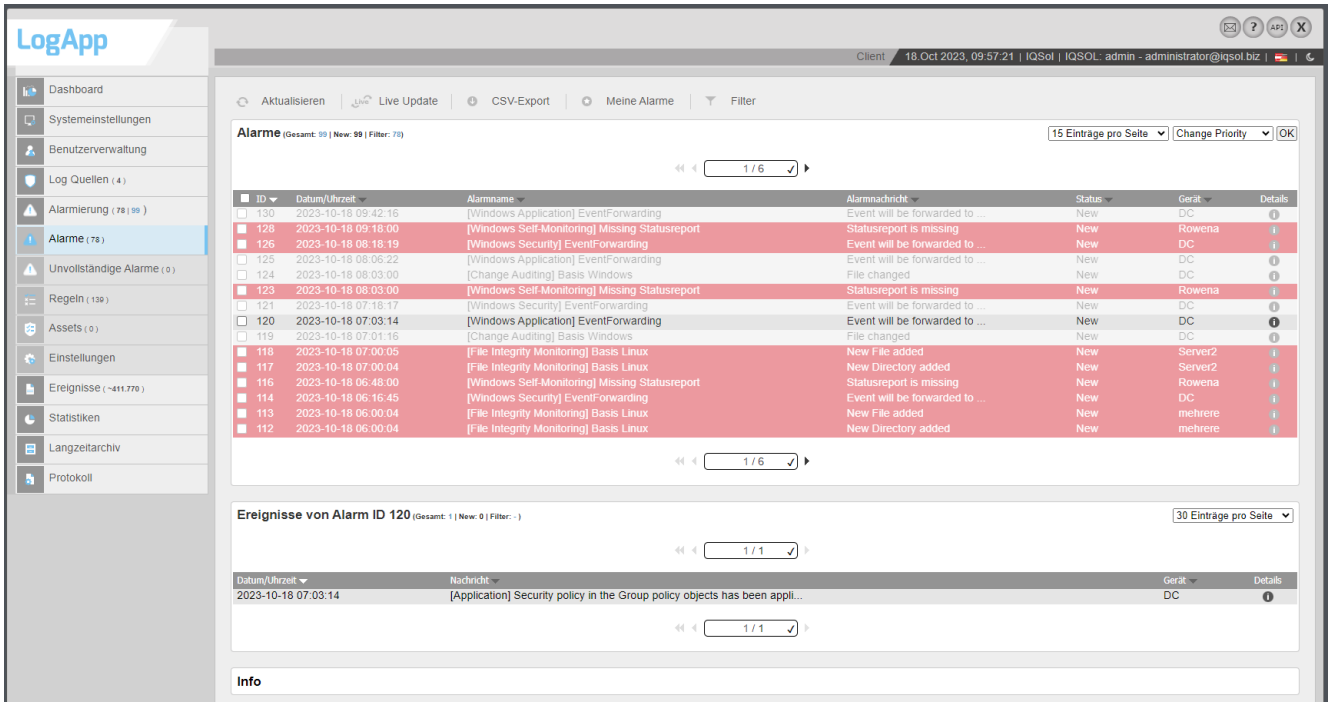

Abbildung 90: Selektierter Alarm mit Ereignissen

Mit den „Details“-Buttons in der Alarmtabelle können Alarme bearbeitet werden. Alarme können Benutzern zugewiesen werden, die per Mail verständigt werden. Priorität und Status des Alarms können verändert werden, und Kommentare können eingetragen werden. Alle Änderungen an Alarmen werden protokolliert und neben „Verlauf“ angezeigt.

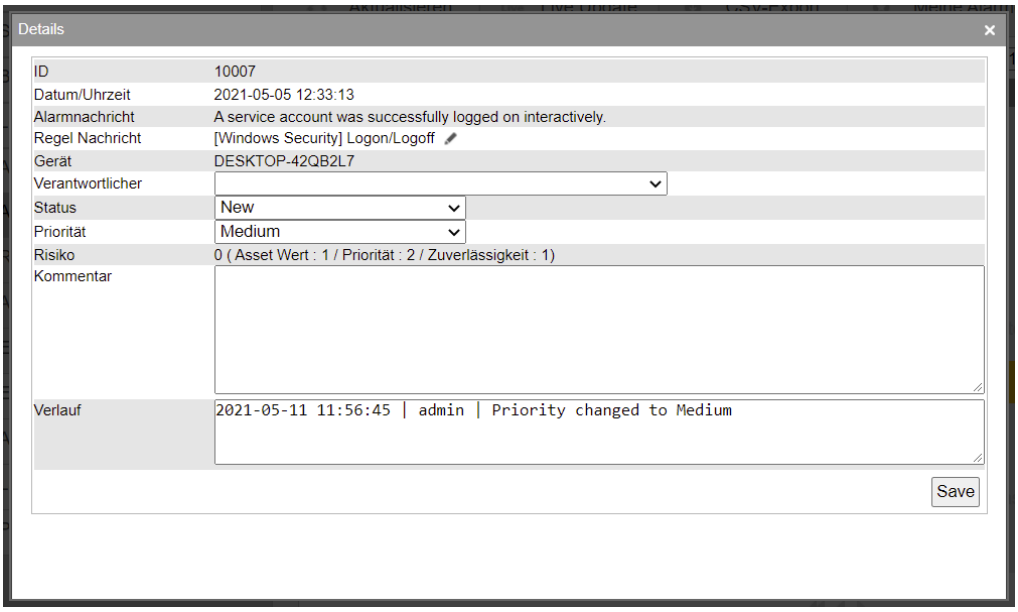

Abbildung 91: Alarmdetails

Der Punkt Priorität gibt die Alarmpriorität an und wird anhand der Definition in der Alarmregel errechnet. Die verschiedenen Prioritäten sind Info, Low, Medium und High. Eine Besonderheit stellt hier die Priorität Info dar. Alarme mit dieser Priorität gelten als Alarmkandidaten. Diese Alarme weisen zwar relevante Ereignisse auf, jedoch nicht in der Zahl/Korrelation, welche für einen Alarm mit niedriger Priorität nötig ist.

Der Punkt „Risiko“ setzt sich aus folgenden Parametern zusammen und wird wie folgt berechnet:

Asset Wert (0-5) x Risikopriorität (0-5) x Zuverlässigkeit (0-10) / 25 = Risiko (0-10)

Der Asset Wert wird in der Asset Verwaltung unter „Alarmierung“ -> „Assets“ zugewiesen. Risikopriorität und Zuverlässigkeit werden in Regeln unter „Alarmierung“ -> „Regeln“ definiert.

Filter für Alarme

Bei den Alarmen gibt es folgende Filtertypen.

Zahlenwertfilter (Filter ID, Risiko)

Diese Filter entsprechen den Zahlenwertfiltern im Bereich der Eventfilter.

Datumsfilter (Filter: Datum/Uhrzeit)

Diese Filter entsprechen den Datumsfiltern im Bereich der Eventfilter.

Gerätefilter (Filter Gerät)

Diese Filter entsprechen den Gerätefiltern im Bereich der Eventfilter.

Statusfilter (Filter Status)

Mit diesem Filter ist es möglich, nur Alarme mit gewissen Status anzuzeigen. Mögliche Werte sind: Alle, Processing, New, Acknowledged, Resolved und Reopened. Es besteht auch die Möglichkeit der Mehrfachauswahl. Der Standardfilter zeigt alle Alarme an, welche nicht Resolved sind

Prioritätenfilter (Filter Priorität)

Der Prioritätenfilter erlaubt es Alarme nur nach gewissen Prioritäten anzuzeigen. Mögliche Werte sind hier Low-High, Info, Low, Medium, High und Alle Prioritäten. Der StandardFilter ist Low-High.

Verantwortlichenfilter (Filter Verantwortlicher)

Bei diesem Filter ist es möglich nach dem Benutzer, welcher bei den Alarmen als Verantwortlicher eingetragen ist zu filtern.

Stringfilter (Filter Alarmname, Alarmnachricht)

Der Stringfilter ist mit dem Algorithmus „Beginnend mit“ implementiert. Als Wildcard dient %. Es können mehrere Werte getrennt durch „ , “ gefiltert werden. Genauere Beschreibungen und Beispiele sind im Anhang „Stringfilter für Alarme“ zu finden.

Wird ein Filter angewandt, so aktualisiert sich der Counter „Filter in der Alarm Überschrift“. Dieser gibt an wie viele Alarme auf den Filter zutreffen.

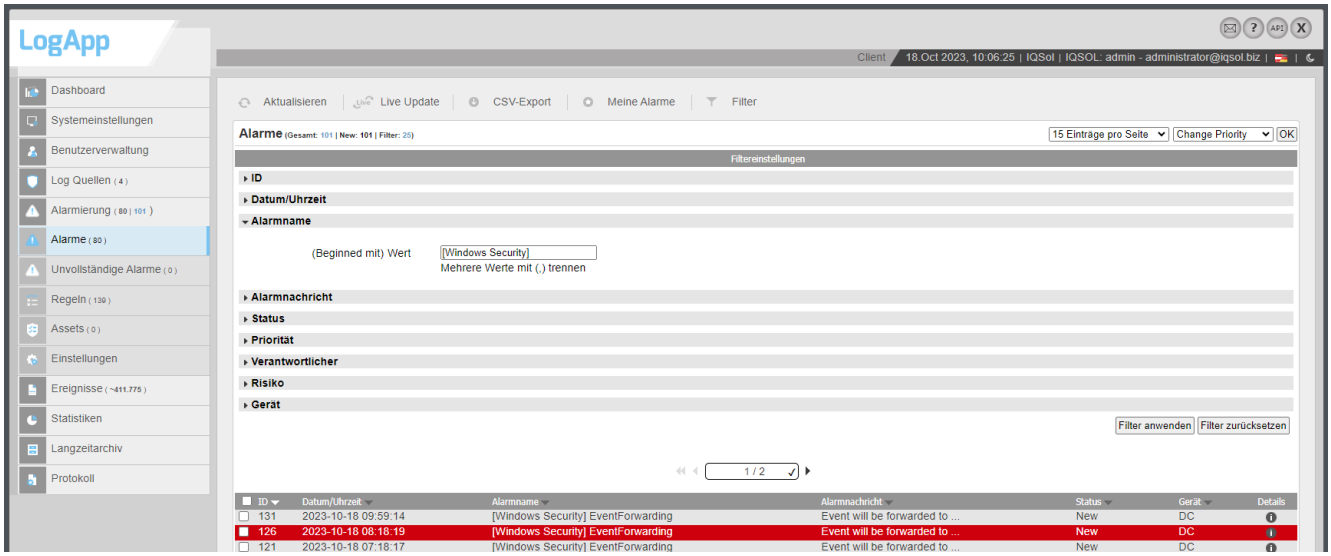

Abbildung 92: Filter Alarme

7.1.2 Unvollständige Alarme

Unvollständige Alarme sind Alarme, welche (noch) keine vollständige Korrelation aufweisen.

In dieser Ansicht stehen Ihnen die gleichen Funktionalitäten wie bei den Alarmen zur Verfügung.

7.1.3 Regeln

Alarmregeln bilden die Grundlage der Korrelation und Alarmierung. Alle eingehenden Ereignisse werden vom AlertParser gegen diese Regeln geprüft. Trifft eine Regel zu, wird ein Alarm erstellt.

Es gibt insgesamt 4 verschiedene Regeltypen:

- Aggregation
- Correlation
- Missing Any
- Missing All

All diese Typen prüfen eingegangene Ereignisse nach gewissen Kriterien. Sind diese Kriterien erfüllt, so wird ein Alarm generiert.

Die zu erfüllenden Kriterien werden mithilfe von relevanten Ereignissen definiert und sind im Kapitel

Definition von relevanten Ereignissen beschrieben.

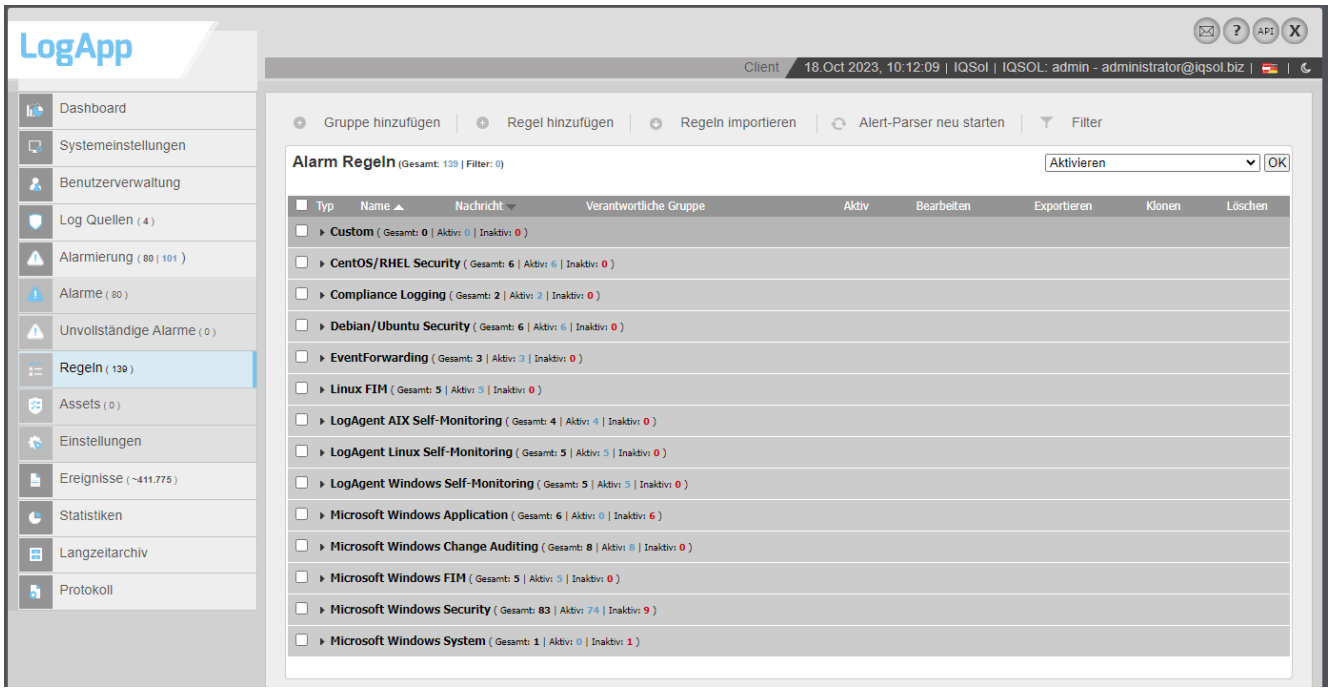

Abbildung 93: Alarmregeln

Allgemeine Einstellungen

Folgende Einstellungen sind für alle AlertRegeltypen gleich.

Option	Beschreibung
Regel	
Aktiv	Aktivieren/Deaktivieren der Alarmregel
Name	Name der Regel
Nachricht	Nachrichtentext zur Beschreibung der Regel
Beschreibung	Beschreibungstext zur detaillierten Beschreibung der Regel
Verantwortliche Gruppe	Benutzergruppe, die bei Alarmen benachrichtigt wird
Regel Gruppe	Regelgruppe, in der die Regel in der Listenansicht angezeigt wird
Konfigurationsgruppen	Konfigurationsgruppen, deren Ereignisse bei der Abarbeitung der Alarmregeln berücksichtigt werden. Bei der Evaluierung der Alarmregeln gegen Ereignisse werden nur Ereignisse betrachtet, die von LogAgents mit den definierten Konfigurationsgruppen stammen.

Aktion	
Lokaler Alarm	Wenn gewählt, wird ein lokaler Alarm erzeugt, falls diese Regel auf Ereignisse anspricht.
Mail Benachrichtigung	Wenn gewählt, wird eine Mailbenachrichtigung erzeugt, falls diese Regel auf Ereignisse anspricht. Für Mailbenachrichtigungen sind Einstellungen unter „System“ -> „E-Mail Einstellungen“ sowie unter „Alarmierung“ -> „Einstellungen“ notwendig.
AMS Benachrichtigung	Wenn gewählt, wird ein AMS-Alarm erzeugt, falls diese Regel auf Ereignisse anspricht. Für AMS-Alarme sind Einstellungen unter „System“ -> „AMS Einstellungen“ (superadmin) sowie unter „Alarmierung“ -> „Einstellungen“ notwendig.
Syslog Benachrichtigung	Wenn gewählt, wird eine Syslog Nachricht an einen Syslog-Dienst versandt, falls diese Regel auf Ereignisse anspricht. Für Syslog Benachrichtigungen sind Einstellungen unter „Alarmierung“ -> „Einstellungen“ notwendig (Zieladresse des Syslog-Servers).
Ereignisweiterleitung	Wenn gewählt, werden jene Ereignisse an eine Ziel-LogApp weitergeleitet, auf welche diese Regel anspricht. Für eine Eventweiterleitung sind Einstellungen unter „Systemeinstellungen“ -> „Grundeinstellungen" notwendig.
REST API Notification	Wenn gewählt, wird bei der Alarmierung ein Webrequest abgesetzt. Die Einstellungen, die den Endpunkt, die Methode, die Header und den Body angeben sind unter Alarmierung -> Einstellungen zu finden.
SNMP Trap Notification	Wenn gewählt, wird bei der Alarmierung ein SNMP Trap gesendet. Die Einstellungen befinden sich Alarmierung -> Einstellungen.
MS Teams Notification	Wenn gewählt, wird bei der Alarmierung eine Nachricht an einen MS Teams Chat oder MS Teams Channel gesendet.
Ausnahmen	
Neue Ausnahme hinzufügen	Hier ist es möglich eine Ausnahme zu definieren. Eine Ausnahme stellt einen Zeitraum dar, in welchem die Alarmregel „inaktiv“ ist und keine Alarme produziert.
Gespeicherte Ausnahmen	Hier sind alle bereits gespeicherten Ausnahmen gelistet. Außerdem ist es möglich, gespeicherte Ausnahmen zu löschen

Aggregation-Regeln

Alarmregeln vom Typ „Aggregation“ lösen einen Alarm aus, wenn mindestens ein eingehendes Ereignis bestimmte Kriterien erfüllt.

Sollten mehrere Relevante Ereignisse definiert werden, so werden diese beim Typ Aggregation mit oder verknüpft.

Folgende Einstellungen können, zusätzlich zu den Allgemeinen Einstellungen, für Regeln vom Typ „Aggregation“ gemacht werden:

Option	Beschreibung
Gruppierung	
Beobachtungszeitraum für die Korrelation (Sekunden)	Hier kann ein eigener Beobachtungszeitraum für die Alarmregel definiert werden. Mit einem Haken bei der entsprechenden Option, kann allerdings auch der globale Beobachtungszeitraum verwendet werden.
Alarmgruppierung	Hier kann gewählt werden, wie die Alarme gruppiert werden. Bei der globalen Gruppierung wird nur ein Alarm pro Beobachtungszeitraum erstellt. Wählt man jedoch die Gruppierung anhand von Feldern, so können unterhalb Felder definiert werden, anhand welcher gruppiert werden sollen. Ereignisse, welche die gleichen Werte in den definierten Feldern vorweisen, werden zu einem Alarm zusammengefasst. Es sind auch Kombinationen mehrerer Felder möglich.
Prio/Reliab. (Priorität/Reliabilität)	
Risikopriorität	Mit diesem Wert lässt sich festlegen, welche Priorität Ereignisse, auf welche diese Regel anspricht, in der Risikowertermittlung grundsätzlich haben (unabhängig von der Quelle der Ereignisse und der Menge der Ereignisse).
Zuverlässigkeit/Alarmpriorität	Entlang der Anzahl der Ereignisse, auf welche im Beobachtungszeitraum die Regel anspricht, kann die Zuverlässigkeit für die Risikobewertung (je mehr Ereignisse, desto zuverlässiger ist die Regel und somit für gewöhnlich höher das Risiko) sowie die Alarmpriorität als Grundlage für die externe Alarmierung festgelegt werden.

Relevante Ereignisse
Ereignisse mit Kriterien, die den Alert auslösen. Einzelne Relevante Ereignisse sind „oder“ verknüpft, einzelne Selektoren „und“ verknüpft und einzelne Übereinstimmungen wieder „oder“ verknüpft Die definierten Ereignisse müssen aus einer im Tab Regel definierten Konfigurationsgruppe kommen. Aus welcher der unter Umständen mehreren Gruppen ist nicht relevant. Sollte jeodch gewünscht sein, dass in einem solchen Fall das Ereignis aus einer bestimmten Konfigurationsgruppe kommt, so kann dies über einen Selektor definiert werden.

Tabelle 24: Aggregation-Regeln

Correlation Regeln

Alarmregeln vom Typ „Correlation“ lösen, genau so wie Aggregation-Regeln, einen Alarm aus, wenn alle definierten Kriterien durch eingegangene Ereignisse erfüllt sind.

Im Unterschied zu Aggregation-Regeln, sind die Relevanten Ereignisse bei diesem Regeltyp jedoch „Und“ verküpft.

Sollte eine Korrelation vollständig sein (für alle relevanten Ereignisse gibt es die Mindestanzahl an relevanten Ereignissen), so wird ein Alarm erstellt.

In der Zwischenzeit wird der Alarm als unvollständiger Alarm geführt und im entsprechenden Menü gelistet.

Kommt während des Beobachtungszeitraumes keine vollständige Korrelation zustande, so bleibt der Alarm ein unvollständiger Alarm.

Während sich der Beobachtungszeitraum bei „Aggregations Regeln“ immer nach dem ersten auftreten eines Relevanten Ergeignisses richtet, so kann sich dieser beim Typ Correlation ändern.

Der Zeitraum richtet sich immer nach dem ältesten N neusten aufgetretenen Ereignis. Wobei N die Mindestanzahl des Ereignisses ist, welches in den Relevanten Ereignissen definiert wird.

Beispiel:

Als Beispiel wird eine Regel angenommen, welche zwei relevante Ereignisse definiert hat (Event A (Mindestanzahl 1) und Event B (Mindestanzahl 1), außerdem gibt es ein Beobachtungszeitfenster von einer Stunde.

Das Fenster wird gestartet indem ein Ereignis vom Typ Event A empfangen wird. Ab diesem Zeitpunkt wird eine Stunde auf ein Event B gewartet. Sollte nun jedoch nach 15 Minuten kein Event B empfangen werden, sondern zwei Events A, so wird der Beobachtungszeitraum aktualisiert und es wird wieder eine Stunde gewartet.

Folgende Einstellungen können, zusätzlich zu den Allgemeinen Einstellungen, für Regeln vom Typ „Aggregation“ gemacht werden:

Option	Beschreibung
Regel	
Priorität	Diese Option gibt an welche Priorität der Alarm haben soll, sollte eine vollständige Korrelation zustandekommen.
Gruppierung	
Beobachtungszeitraum für die Korrelation (Sekunden)	Hier kann ein eigener Beobachtungszeitraum für die Alarmregel definiert werden. Mit einem Haken bei der entsprechenden Option, kann allerdings auch der globale Beobachtungszeitraum verwendet werden.
Alarmgruppierung	Hier kann gewählt werden, wie die Alarme gruppiert werden. Bei der globalen Gruppierung wird nur ein Alarm pro Beobachtungszeitraum erstellt. Wählt man jedoch die Gruppierung anhand von Feldern, so können unterhalb Felder definiert werden, anhand welcher gruppiert werden sollen. Ereignisse, welche die gleichen Werte in den definierten Feldern vorweisen, werden zu einem Alarm zusammengefasst. Es sind auch Kombinationen mehrerer Felder möglich.
Relevante Ereignisse	
Ereignisse mit Kriterien, die den Alert auslösen. Einzelne Relevante Ereignisse sind „und“ verknüpft, einzelne Selektoren „und“ verknüpft und einzelne Übereinstimmungen „oder“ verknüpft Die definierten Ereignisse müssen aus einer im Tab Regel definierten Konfigurationsgruppe kommen. Aus welcher der unter Umständen mehreren Gruppen ist nicht relevant. Sollte jedoch gewünscht sein, dass in einem solchen Fall das Ereignis aus einer bestimmten Konfigurationsgruppe kommt, so kann dies über einen Selektor definiert werden. Außerdem ist es beim Typ Correlation möglich eine Mindestanzahl an Ereignissen zu definieren, welche angibt, wieviele Ereignisse des Relevanten Ereignisses für eine vollständige Korrelation benötigt werden.	

Tabelle 25: Correlation-Regeln

Missing All

Alarmregeln vom Typ „Missing All“ lösen einen Alarm aus, wenn ein erwartetes Ereignis nicht innerhalb einer festgelegten Zeitspanne eintrifft.

Sollten mehrere relevanten Ereignisse definiert sein, so wird ein Alarm nur erstellt, wenn alle relevanten Ereignisse fehlen.

Folgende Einstellungen können zusätzlich für Regeln vom Typ „Missing All“ gemacht werden:

Option	Beschreibung
Regel	
Korrelation	Hier wird definiert wie der „Missing Alarm“ gruppiert wird. Hierbei gibt es drei verschiedene Möglichkeiten. • **Globale Korrelation**: betrachtet für die Regel alle Geräte, d.h. bei Zutreffen der Kriterien werden Ereignisse von allen Geräten zugeordnet. • **Pro-Gruppen Korrelation**: betrachtet für die Regel alle Geräte der zugeordneten Gerätegruppe, d.h. bei Zutreffen der Kriterien werden Ereignisse von allen Geräten innerhalb einer Gerätegruppe zugeordnet. • **Pro-Gerät Korrelation**: erzeugt einen Alarm pro Gerät.
Priorität	Definiert die Priortät, mit welcher der Alarm angelegt werden soll
Minute	Minute, zu der das Event erwartet wird
Stunde	Stunde, zu der das Event erwartet wird, * für jede Stunde
Tag des Monats	Tag des Monats, an dem das Event erwartet wird, * für jeden Tag
Monat	Monat, in dem das Event erwartet wird, * für jeden Monat
Tag der Woche	Tag der Woche, an dem das Event erwartet wird, 1 für Montag bis 7 für Sonntag, * für jeden Tag
Zeitfenster in Minuten	Zeitfenster in Minuten ab der konfigurierten Uhrzeit, in dem das Event eintreffen muss

Relevante Ereignisse
Ereignisse mit Kriterien, die den Alert auslösen. Tritt keines der definierten Ereignisse auf, so wird ein Alarm ausgelöst. Die definierten Ereignisse müssen aus einer im Tab Regel definierten Konfigurationsgruppe kommen. Aus welcher der unter Umständen mehreren Gruppen ist nicht relevant. Sollte jeodch gewünscht sein, dass in einem solchen Fall das Ereignis aus einer bestimmten Konfigurationsgruppe kommt, so kann dies über einen Selektor definiert werden.

Tabelle 26: Missing-All-Regeln

Missing Any

Alarmregeln vom Typ „Missing Any“ entsprechen im Wesentlichen dem Typ „Missing All“, jedoch mit dem Unterschied, dass der Alarm ausgelöst wird sollte bereits eines der, unter Umständen mehreren, relevanten Ereignissen fehlen. (Im Gegensatz zu einer Missing All Regel, welche nur alarmiert, wenn alle Ereignisse fehlen)

Definition von relevanten Ereignissen

Relevante Ereignisse in Alarmregeln definieren, welche Ereignisse beim Auftreten bzw. Nicht-Auftreten innerhalb der angegebenen Zeitspanne, einen Alarm auslösen.

Mit dem Plus-Symbol kann ein neues Ereignis angelegt werden. Je nachdem, welcher Regeltyp verwendet wird, werden mehrere Relevante Ereignisse mit „und“ oder „oder“ verknüpft.

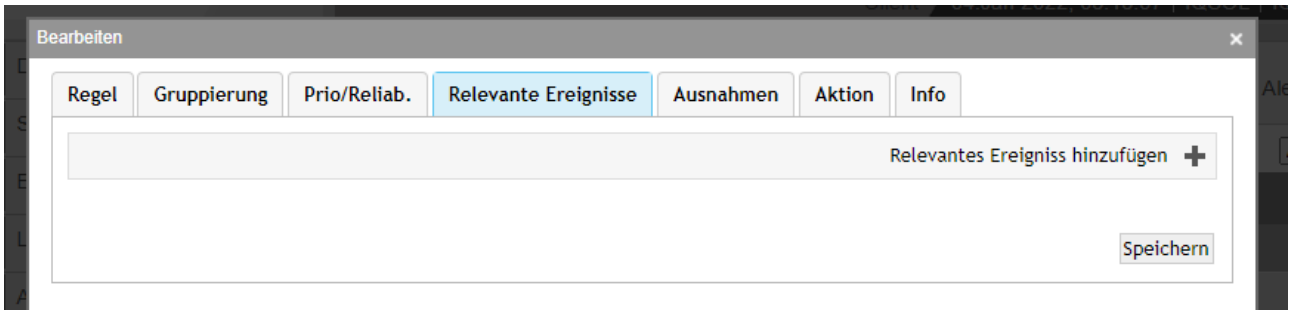

Abbildung 94: Eintragen eines relevanten Ereignisses

Für eingetragene Ereignisse kann ein Name oder eine Beschreibung im Textfeld eingetragen werden. Mit den Symbolen links unten können für das Ereignis Kriterien eingetragen oder gelöscht werden.

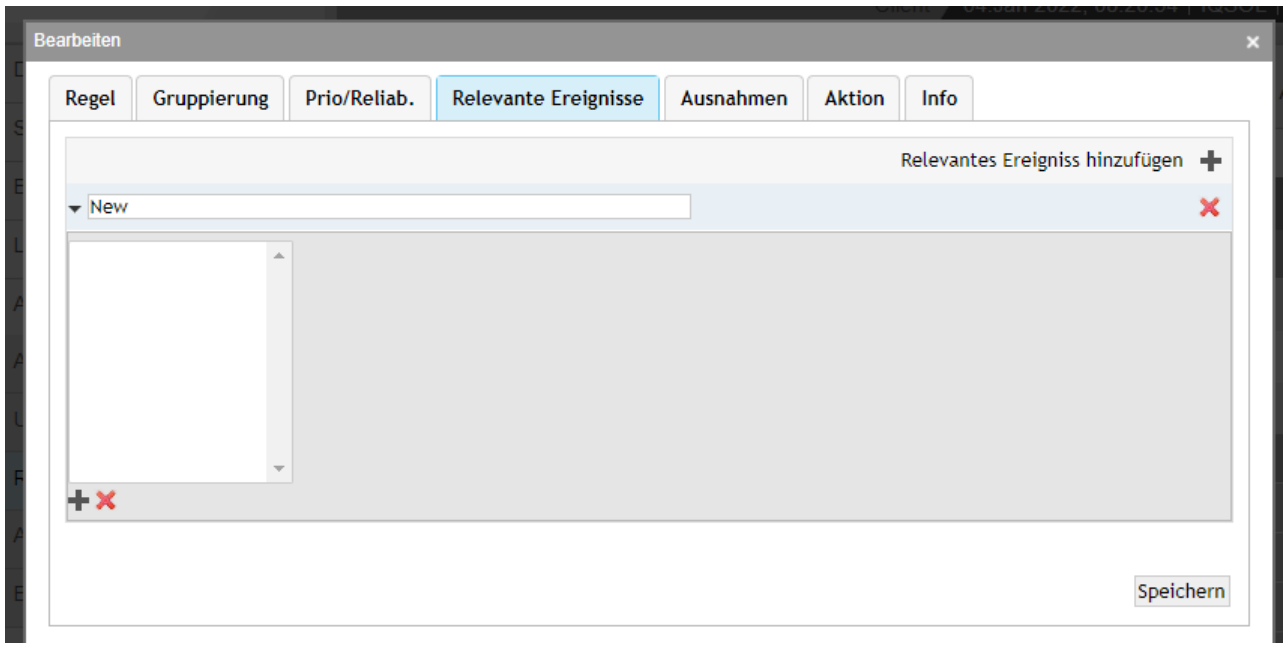

Abbildung 95: Relevantes Ereignis

Kriterien stellen Datenbankspalten dar, deren Inhalt überprüft wird. Die Datenbankspalten können als Selektor Typ ausgewählt werden und mit den Operationen „equals“ und „not equals“ für einfache Vergleiche oder „RegEx“ für die Verwendung von Regular Expressions mit festgelegten Werten verglichen werden. Werden mehrere möglich Werte angegeben, werden diese mit einem logischen ODER verknüpft.

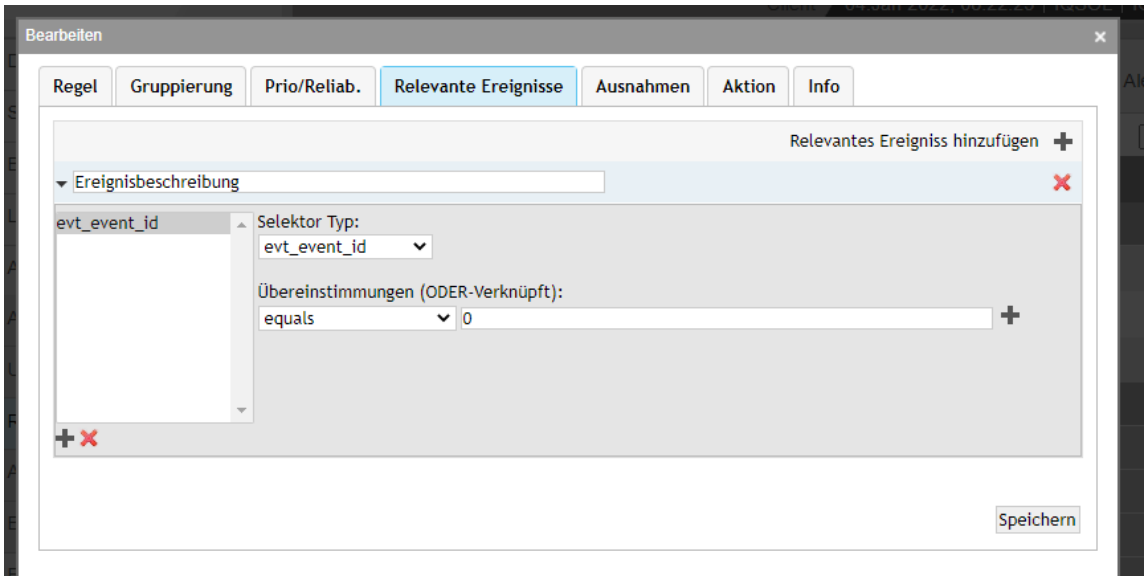

Abbildung 96: Anlegen eines Selektors

Die in der folgenden Abbildung dargestellte Beispielregel für den Alarm „Audit Log was cleared“ würde aufgrund der festgelegten Kriterien (evt_event_id equals „1102“ UND log_reference equals „Security“) für das nachfolgend abgebildete Ereignis einen Alarm auslösen.

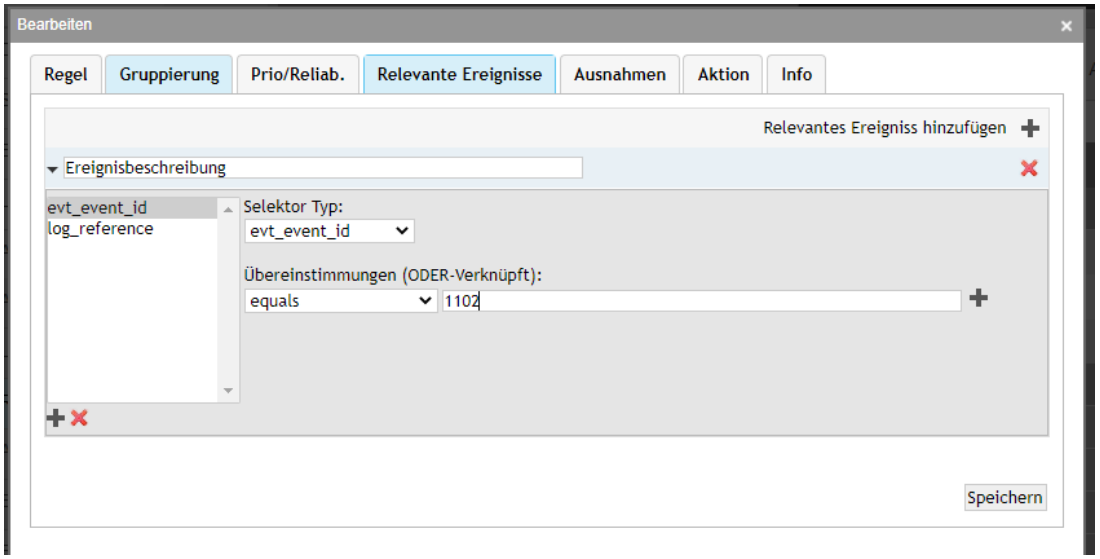

Abbildung 97: Ereignisdefinition

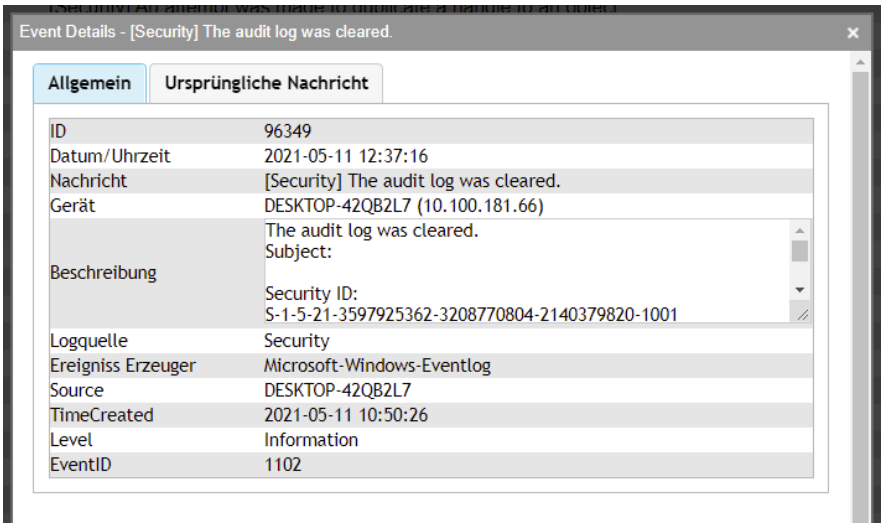

Abbildung 98: Windows Security Ereignis EventID 1102

In der nachfolgenden Abbildung ist eine komplexere Aggregation Alarmregel dargestellt, die ein Windows Security Ereignis mit der evt_event_id „4625“ oder ein FortiGate Ereignis mit der evt_msg_short „Attack detected“ ODER „Virus detected“ als Regular Expression erwartet.

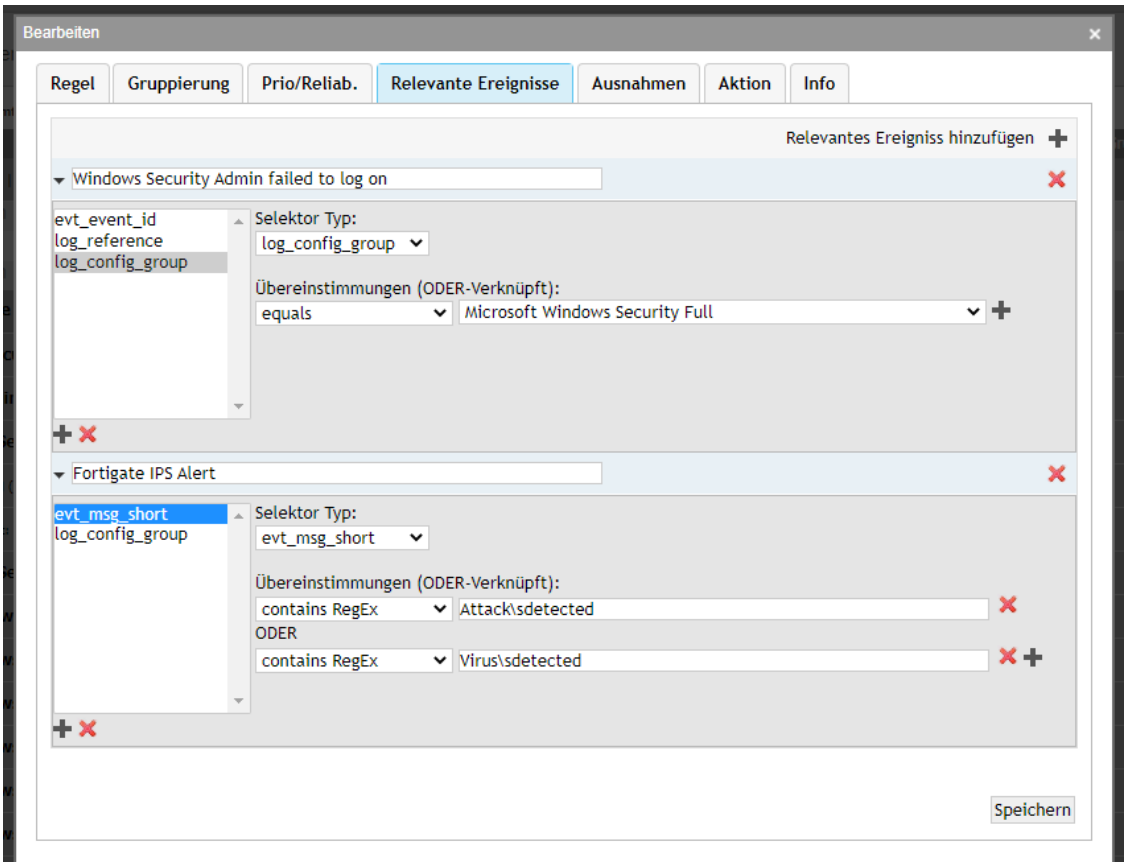

Abbildung 99: Verknüpfung von zwei Ereignissen

Würden diese Relevanten Ereignisse in einer Alarmregel vom Typ Correlation definiert werden, so müsste für einen vollständigen Alarm ein Security Ereignis mit der evt_event_id „4625“ und ein FortiGate Ereignis mit der evt_msg_short „Attack detected“ ODER „Virus detected“ als Regular Expression Match eingegangen sein.

Exportieren von Regeln

Um Alertregeln zu sichern und gegebenenfalls auf anderen LogApps wiederverwenden zu können, ist es möglich diese zu exportieren. Um Regeln zu exportieren können Sie entweder jede Regel einzeln oder mehrere per Bulkoperation exportieren.

Wird die Aktion gestartet erscheint folgender Dialog.

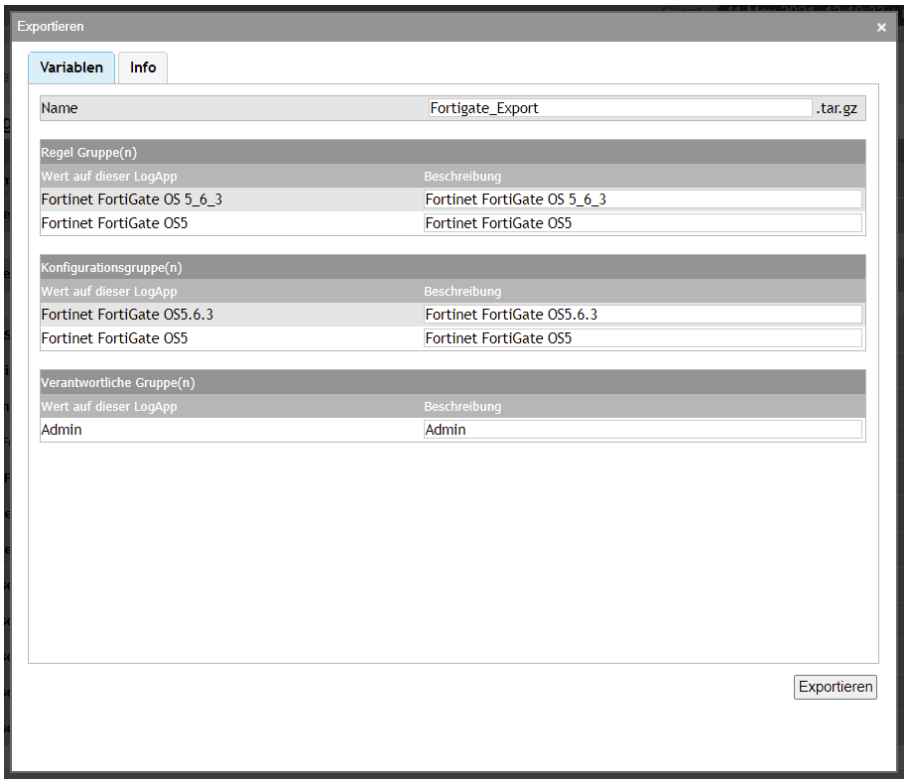

Abbildung 100 Export von Alarmregeln

In diesem Dialog bietet sich die Möglichkeit Beschreibungen für Regelgruppen, Konfigurationsgruppen und verantwortliche Gruppen zu hinterlegen. Da diese 3 Eigenschaften nicht bei jeder LogApp gleich benannt sein müssen, kann hier eine Beschreibung festgelegt werden, welche Standardmäßig dem aktuellen Namen entspricht. Bei einem Reimport wird dann versucht Werte auf der importierenden LogApp zu finden, welche dieser Beschreibung entsprechen.

Import von Regeln

Mit der Schaltfläche Regeln importieren ist es möglich vorher bereits exportierte Alarmregeln zu importieren.

Nach dem Klick auf „Regeln importieren“ und der anschließenden Auswahl des zu importierenden Archivs, erscheint ein Fenster mithilfe dessen Sie Einstellungen zum Import treffen können.

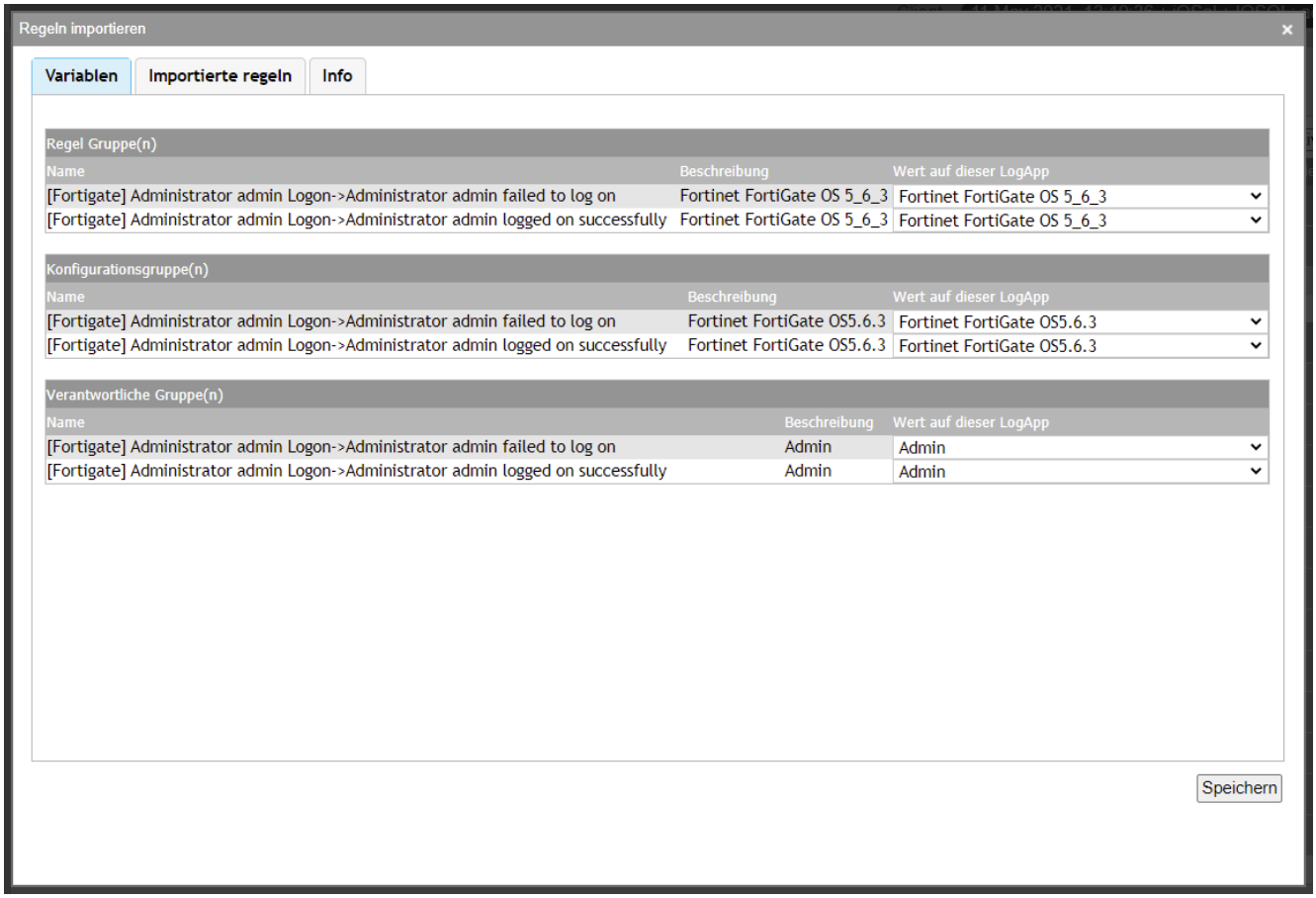

Abbildung 101 Import Alarmregeln Tab 1

Im ersten Tab lassen sich die Regel Gruppen, Konfigurationsgruppen und verantwortlichen Gruppen zuweisen.

Hierbei versucht die LogApp die entsprechenden Werte, welche in den Beschreibungen des Exports definiert sind, zu identifizieren und die richtigen Werte zuzuordnen. Sollte diese Zuordnung nicht korrekt sein, da die entsprechenden Gruppen nicht existieren oder jetzt ein anderer Wert verwendet werden soll, so kann dies über das Dropdown geändert werden.

Welche Regeln importiert oder aktualisiert werden sollen, lässt sich im zweiten Tab festlegen.

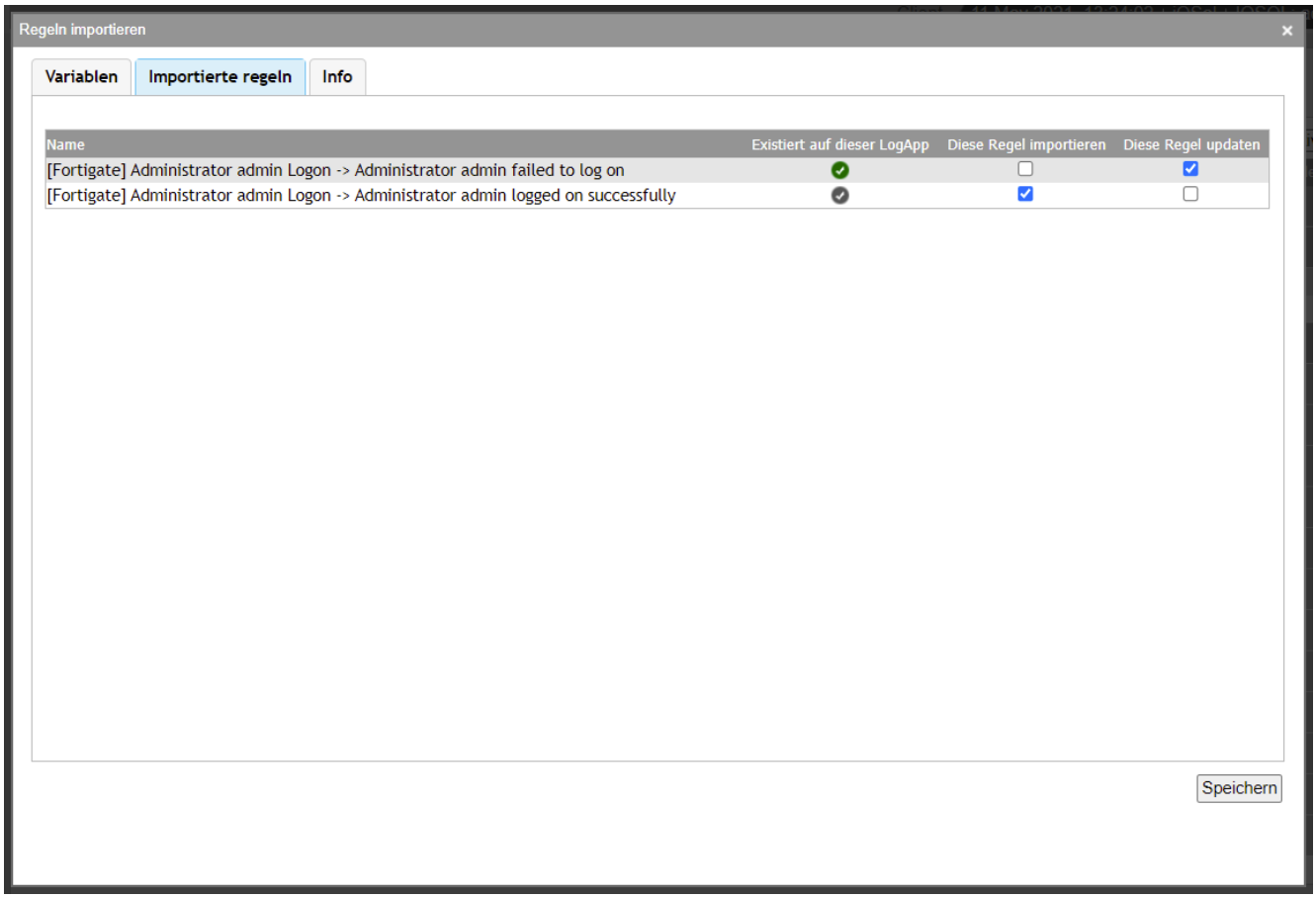

Abbildung 102 Import Alarmregeln Tab 2

Hier werden ident zu den Konfigurationsgruppen alle im Export enthaltenen Regeln aufgelistet und angezeigt ob sie auf der LogApp bereits existieren. Mit den Checkboxen kann entschieden werden ob die Alarmregel importiert oder falls bereits existent upgedatet werden soll. Sollte eine Regel bereits existieren und es wird die Regel importieren Aktion gewählt, so wird eine neue Regel angelegt mit dem Suffix _import.

7.1.4 Assets

In der Ansicht Assets werden alle bekannten Geräte (Logquellen) angezeigt. Zusätzlich können manuell Assets angelegt werden, um eine Risikobewertung auch für Assets durchführen zu können, die als Quelle oder Ziel in Ereignissen protokolliert werden, selbst aber keine Log-Quelle für LogApp darstellen.

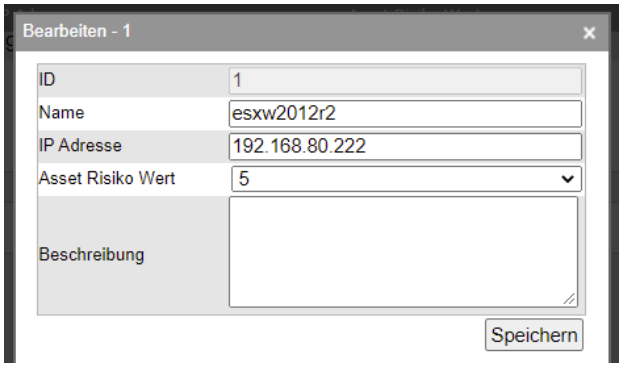

Abbildung 103: Detailansicht Asset

Für die weiterführende Risikobewertung in Alarmen ist es notwendig, jedem Asset einen entsprechenden Risikowert zuzuordnen (0 … kein Risiko, 3 … mittleres Risiko, 5 … höchstes Risiko), welcher die Gefährdung eines Assets widerspiegelt.

7.1.5 Einstellungen

Unter „Einstellungen“ können die Benachrichtigungsoptionen bearbeitet werden.

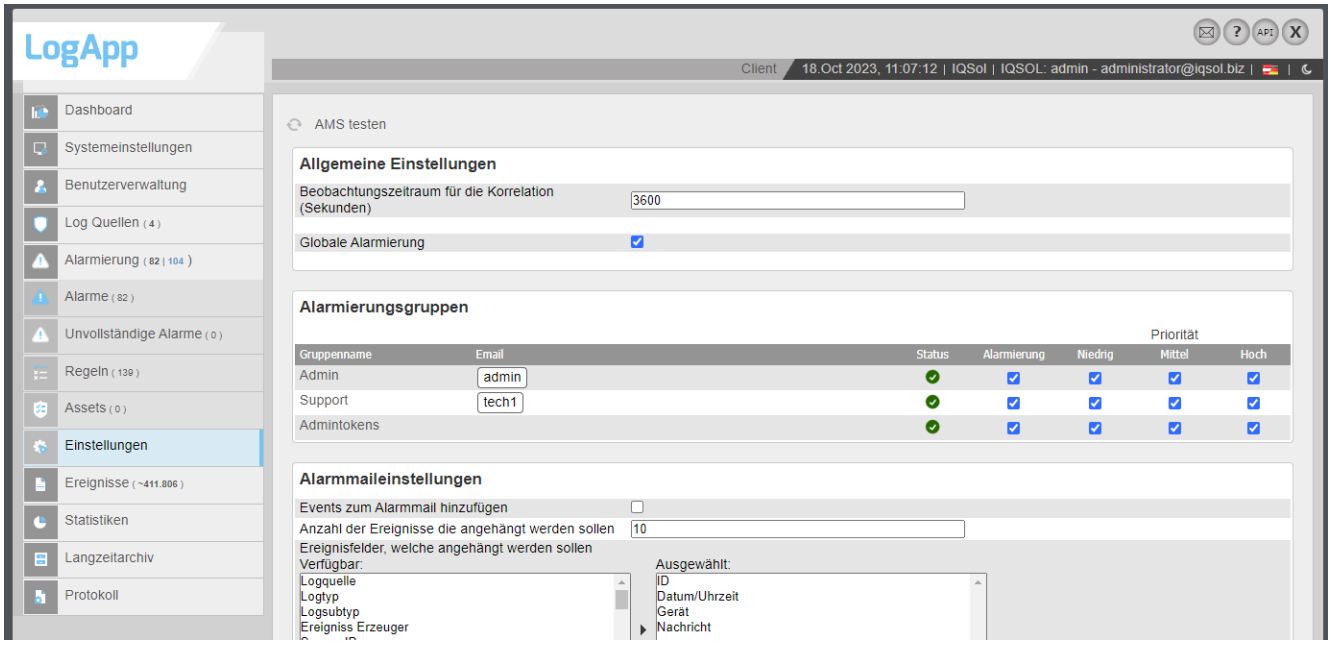

Abbildung 104: Alarmierungseinstellungen

Allgemeine Einstellungen

Wenn die Option „Globale Alarmierung“ (siehe 6.2.2 Grundeinstellungen) deaktiviert ist, wird jeweils die in der Alarmregel eingetragene Benutzergruppe benachrichtigt, anderenfalls werden alle Benutzergruppen entsprechend der Alarmierungseinstellungen benachrichtigt.

Der Beobachtungszeitraum steuert jene Zeitdauer, innerhalb welcher Ereignisse demselben Alarm zugordnet werden. Als Startzeitpunkt wird das Eintreffen des ersten relevanten Ereignisses bzw. die Anlage des Alarms selbst angenommen. Nach Ablauf des Beobachtungszeitraumes wird zwingend ein neuer Alarm angelegt, um auch alle aktivierten weiterführenden Alarmierungsmechanismen erneut auszulösen.

Alarmierungsgruppen

In der Liste der Alarmierungsgruppen werden automatisch alle vorhandenen Benutzergruppen angezeigt. Für jede Gruppe kann mit den Kontrollkästchen die Benachrichtigung aktiviert bzw. deaktiviert und nach Priorität selektiert werden. Gruppen, die in der Benutzerverwaltung deaktiviert wurden, werden grau angezeigt und sind von der Alarmierung ausgenommen.

Die Alarmierung per E-Mail setzt voraus, dass ein gültiger Mail Server konfiguriert wurde (siehe 6.2.3 E-Mail Einstellungen).

Alarmmaileinstellungen

Diese Einstellungen ermöglichen das Konfigurieren der Alarmmail. Mithilfe der entsprechenden Optionen kann entschieden werden ob Events an die E-Mail angehängt werden, wie viele es maximal sein sollen und welche Spalten dargestellt werden sollen.

AMS

Wurden unter den AMS Einstellungen (siehe Abschnitt 5.2.10) alle notwendigen Einstellungen durchgeführt, kann für die Alarmierung auch der Alert Messaging Server (AMS) herangezogen werden. Dadurch ist es möglich, E-Mail, SMS und oder Voice für die Alarmierung zu verwenden. Je nach Priorität kann die entsprechende Option gesetzt werden. Den Namen der Störungskategorie kann schnell und einfach aus der AMS Weboberfläche bezogen werden.

Syslogweiterleitung

Im Abschnitt Syslogweiterleitung werden alle notwendigen Parameter für einen Versand eines Alarmes als Syslognachricht an einen Syslogdienst definiert.

Verfügbare Parameter zur Konfiguration sind:

- Aktiv: aktiviert die Syslogweiterleitung.
- Zieladresse/Zielport: Adresse/Port zu welcher der Alarm als Syslogmessage weitergeleitet wird.
- Sende Alarme mit der Priorität: Diese Checkboxen geben an, dass nur Alarme mit den ausgewählten Prioritäten weitergeleitet werden

Wird ein Alarm nun weitergeleitet, so wird eine Syslognachricht im Key/Value Format versendet. Folgende Parameter werden in dieser Nachricht versendet:

"AlertName":"[NAME_OF_ALERT]";"TimeStamp":"[TIMESTAMP_OF_ALERT]";"Message":"[MESSAGE_OF_ALERT]";"Owner":"[OWNER_OF_ALERT]";"Hosts":"[AFFECTED_HOSTS]";"Priority":"[PRIORITY_OF_ALERT]";"GUI-Reference":"[MANAGEMENT_ADDRESS_OF_LOGAPP]";"Client":"[CLIENTNAME_OF_LOGAPPCLIENT]";

Beispiel einer Syslognachricht:

"AlertName":"[Windows Security] Logon/Logoff";"TimeStamp":"04.07.2019 08:33:53";"Message":"An administrator account failed to log on.";"Owner":"admin";"Hosts":"LADevHost1";"Priority":"Low";"GUI-Reference":"https://10.100.181.10";"Client":"iqsol";

REST API Weiterleitung

Im Widget REST API Weiterleitung können die erfoderlichen Einstellungen vorgenommen werden, um Alarme als Webrequests weiterzuleiten.

Hier können sowohl eine URI als auch die http-Methode angegeben werden.

Im Bereich der Header können header definiert werden und mit dem + Button hinzugefügt werden. Wird die Checkbox geheim aktiviert, so wird der inhalt des Headers verteckt/verschlüsselt, dies empfiehlt sich für Authentifizierungsheader.

Im Body-Bereich kann der zu sendende Requestbody angegeben werden.

Sowohl im Body als auch bei den Headern können Parameter im String verwendet werden, welche beim Senden des Requests durch konkrete Werte des Alarms ersetzt werden.

Mögliche Variablen:

- @alertName: dieser String
- @alertMessage
- @alertID
- @eventCount
- @alertPriority
- @eventMessage1
- @eventDescription1
- @affectedDevice1
- @eventMessage2
- @eventDescription2
- @affectedDevice3
- @eventMessage3
- @eventDescription3
- @affectedDevice3

MS Teams Weiterleitung

Mit diesen Einstellungen wird festgelegt, wie und an welchen Channel oder welches Team gesendet werden soll. Die einzelnen Variablen müssen mit diversen Webrequests abgeholt werden. Hierzu konsultieren sie bitte das Extradokument „MSTeams Notification konfigurieren“.

In der zu sendenden Nachricht ist es möglich die gleichen Parameter zu verwenden wie bei der REST API Weiterleitung.

SNMP Trap Weiterleitung

Mit diesen Einstellungen wird festgelegt wie ein Alarm als SNMP Trap weitergeleitet wied, falls aktiviert.

Es ist möglich die Weiterleitung zu aktivieren und Host und Port zu spezifizieren, sowie den Enterpriseidentifier zu definieren.

Die SNMP Variablen können in der Zeile SNMP Variablen festgelegt werden. Hier können für die Variablenwerte die gleichen Parameter verwendet werden, wie beim MS Teams und bei der REST Weiterleitung.

Anschließend kann noch festgelegt werden ob ein SNMP v2 oder v3 Trap gesendet wird, mit den dazugehörigen Authentifizierungsinformationen.

7.2 Ereignisse

7.2.1 Übersicht

Unter „Ereignisse“ werden die Ereignisse von Hosts (v.a. Server) und Netzwerk-Geräten (z.B. Switches, Firewalls). Über die Menüpunkte können entweder alle Ereignisse oder nach den Kategorien gefilterte Ereignisse angezeigt werden.

Die Buttons im oberen Bereich der Seite ermöglichen das Aktualisieren, Exportieren und Filtern der Ereignisse.

Beachten Sie, dass die Filterfunktionen, je nach Anzahl der gespeicherten Ereignisse, längere Zeit dauern können. Filter können mit dem Button „Ansicht zurücksetzen“ zurückgesetzt werden.

Über die Schaltfläche „CSV-Export“ lassen sich alle Events welche auf den aktuellen Filter zutreffen exportieren. Je nach gesetztem Filter kann dies zu längeren Wartezeiten und größeren Files führen.

Sind mehr als 10.000 Ereignisse vorhanden, so wird kein Export generiert. Mithilfe der Filterfunktion können die Ereignisse eingegrenzt werden um die Anzahl zu reduzieren und danach einen Export zu erstellen.

Wird das „Live Update“ – Icon in Farbe angezeigt, so ist dies aktiviert und die Ereignisse werden in einem vorgegebenen Intervall stetig aktualisiert. Ist das Icon grau, so ist das Live Update deaktiviert.

Mit dem Button „Einstellungen“ ist es möglich, die Spalten der Listenansicht zu ändern. Es kann definiert werden, welche Details für die Events angezeigt werden.

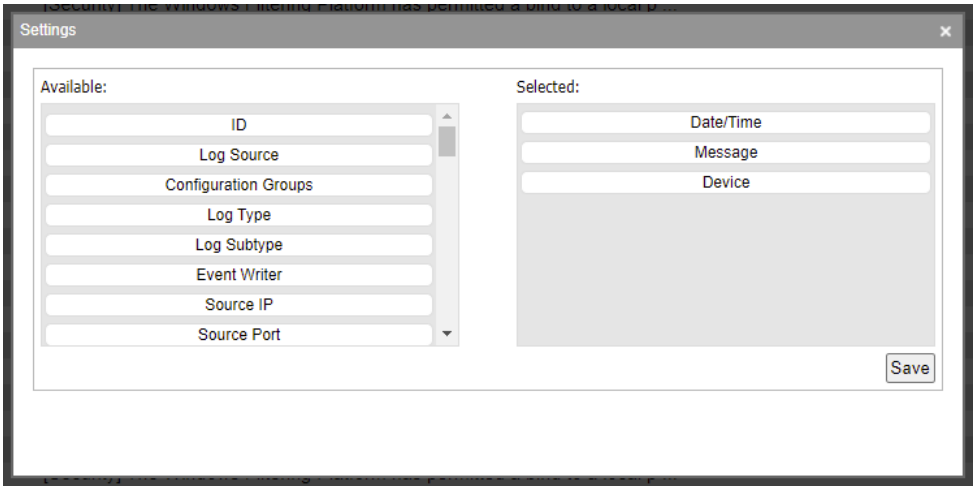

Abbildung 105: Ereigniseinstellungen

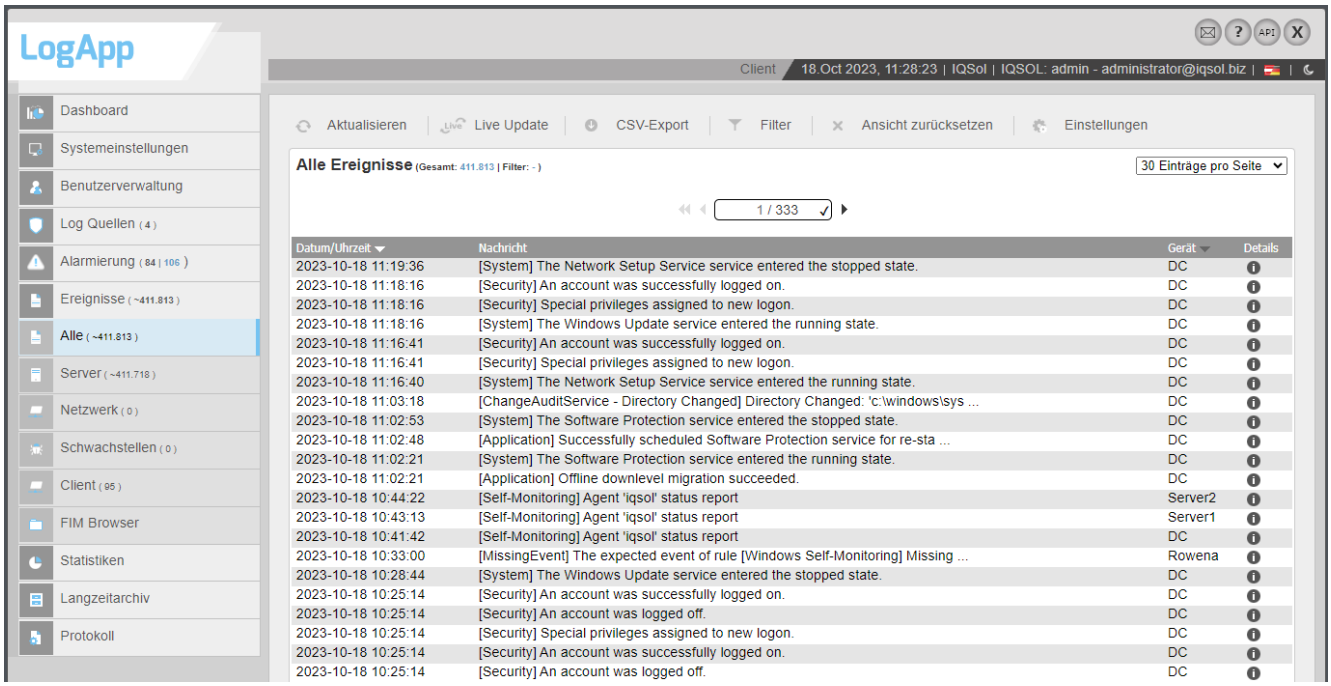

Abbildung 106: Ereignisse

Mit den „Details“-Buttons in der Listenansicht können die Ereignis-Details angezeigt werden.

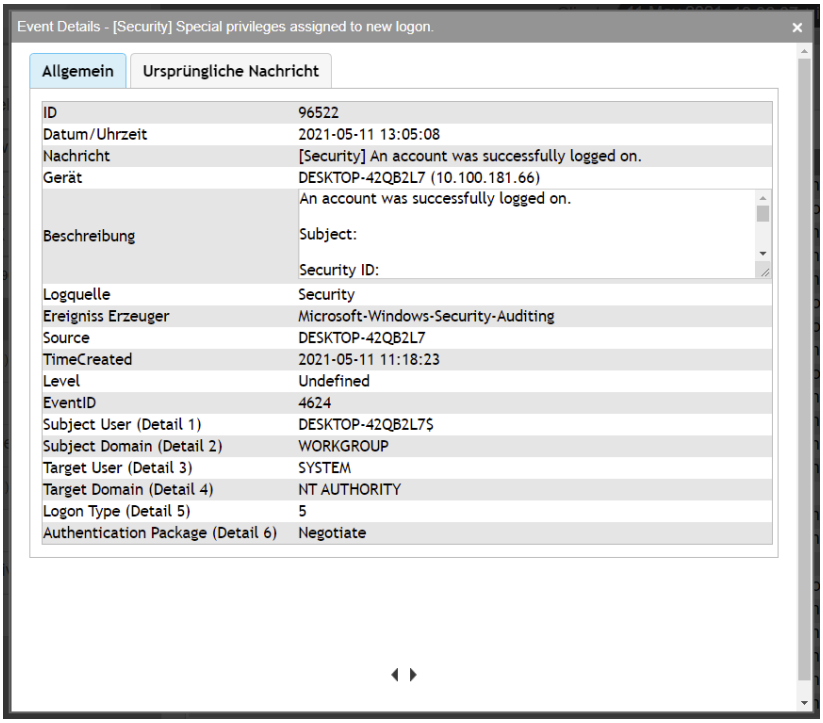

Abbildung 107: Ereignis-Details

7.2.2 Eventfilter

Als Filter stehen alle in der Eventansicht einzusehenden Spalten zur Verfügung, diese lassen sich in sechs verschiedene Typen einteilen:

- Datumsfilter
  Bei einem Datumsfilter lässt sich entweder nach Tagen (heute, letzten 7 Tage, etc.) oder nach einem konkreten Zeitraum filtern. Hierbei zählt jeweils die über die Checkbox gewählte Version.
- Stringfilter (Keyword)
  Bei Stringfiltern wird mithilfe von RegEx gefiltert. Hierbei muss darauf geachtet werden, dass standardmäßig davon ausgegangen wird, dass der Anfang der RegEx auch den Anfang eines Wortes darstellt. Optional können auch, getrennt durch einen Beistrich, mehrere Werte eingegeben werden, diese werden mit oder verknüpft.
  Diese Filter werden bei allen Stringfeldern angewandt außer Nachricht, Beschreibung und Raw Message
- Stringfilter (Fulltext):
  Bei den Fulltextfiltern kann mithilfe einer speziellen Beschreibungssprache gefiltert werden. Hierbei wird der Filter in terms umgewandelt (aufgesplittet anhand von Leerzeichen). Die Reihenfoge der Terms ist dabei nicht relevant, so matched ein Filter mit dem Wert `Logon Success` sowohl auf die Nachricht `Logon was a Success` als auch auf die Nachricht `Logon Success for Admin`. Sollte der Filter exact so als Phrase angewandt werden sollen, so ist sie unter doppelte Anführungszeichen zu setzen (z.B. „Logon Success for“). Außerdem sind noch andere spezielle Wildcards möglich (Genaueres dazu siehe Beispiele für Stringfilter bei Events)
- Zahlenwertfilter
  Zahlenfilter können sowohl mit ganzen Zahlen, als auch mit Zahlenbereichen verwendet werden. Dieser Filtertyp unterstützt auch eine Negierung.
- Gerätefilter
  Mit dem Gerätefilter können Ereignisse nach einem oder mehreren Devices gefiltert werden.
- Konfigurationsgruppenfilter
  Mit dem Konfigurationsgruppenfilter können Ereignisse nach einer oder mehreren Konfigurationsgruppen gefiltert werden.

Diese Filter können beliebig kombiniert werden. Einzelne Filter werden immer und verknüpft.

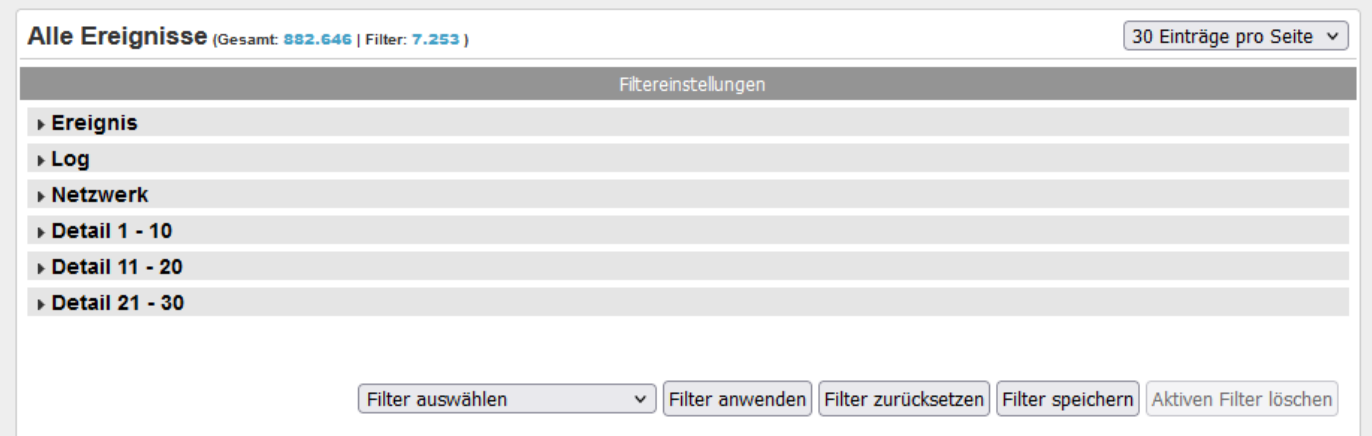

Abbildung 108: Ereignis-Filter

Wird ein Filter angewandt, so wird der Counter Filter in der Überschrift aktualisiert. Dieser zeigt dann die Anzahl der Events, welche vom Filter zurückgeliefert werden. Sollten keine Ereignisse auf den Filter zutreffen oder alle Ereignisse zutreffen, so wird bei Filter – angezeigt.

Beispiele für die Filtermöglichkeiten von Stringfiltern und Zahlenwertfiltern sind im Anhang „Beispiele für Filter bei Events“.

Über die Filtereinstellungen im Menüpunkt „Alle Ereignisse“ können Filter abgespeichert werden.

Um einen Filter abzuspeichern muss dieser manuell gesetzt und angewendet werden. Mit einem Klick auf den Button „Filter speichern“ kann der aktive Filter gespeichert werden.

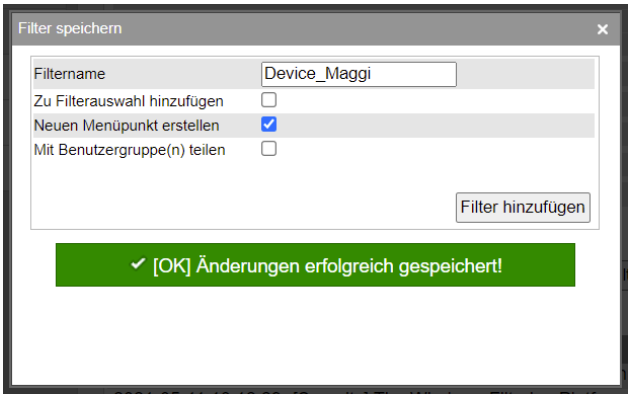

Abbildung 109: Filter speichern

Bei der Speicherung des Filters kann folgendes gewählt/vergeben werden:

Option	Beschreibung
Filter speichern	
Filtername	Ein Name für den Filter muss vergeben werden
Zu Filterauswahl hinzufügen	Filter wird im Menüpunkt „Alle Ereignisse“ gespeichert und steht in einer Selectbox zur Auswahl zur Verfügung
Neuen Menüpunkt erstellen	Ein neuer Menüpunkt wird erstellt und erscheint als Unterkategorie im Hauptmenü „Ereignisse“.
Mit Benutzergruppe(n) teilen	Filter kann mit selektierten Benutzergruppen geteilt werden.

Tabelle 27: Eventfilter speichern

Wird ein Filter aus der Selectbox angewandt, kann dieser weiter gefiltert werden. Hierfür werden weitere Filter aus der Filterauswahl zusätzlich zum gespeicherten Filter ausgewählt und mit dem Button „Filter anwenden“ aktiviert. Der „Filter anwenden“ – Button aktiviert sowohl manuelle Filter als auch jene aus der Selectbox.

Nach jeder Filterung sollten die Filter mit dem „Filter zurücksetzen“- Button zurückgesetzt werden bevor erneut gefiltert wird, da sonst die Ergebnisse möglicherweise nicht korrekt angezeigt werden.

Auch bei einem selbst erstellten Menüpunkt ist diese Art der Filterung möglich.

Soll ein gespeicherter Filter der Selectbox gelöscht werden, so aktiviert man diesen und klickt anschließend auf den „Aktivierten Filter löschen“ - Button welcher bei nicht aktivem Filter deaktiviert ist.

Bei einem neu erstellten Menüpunkt kann dieser durch einen Klick auf „Filter löschen“ gelöscht werden.

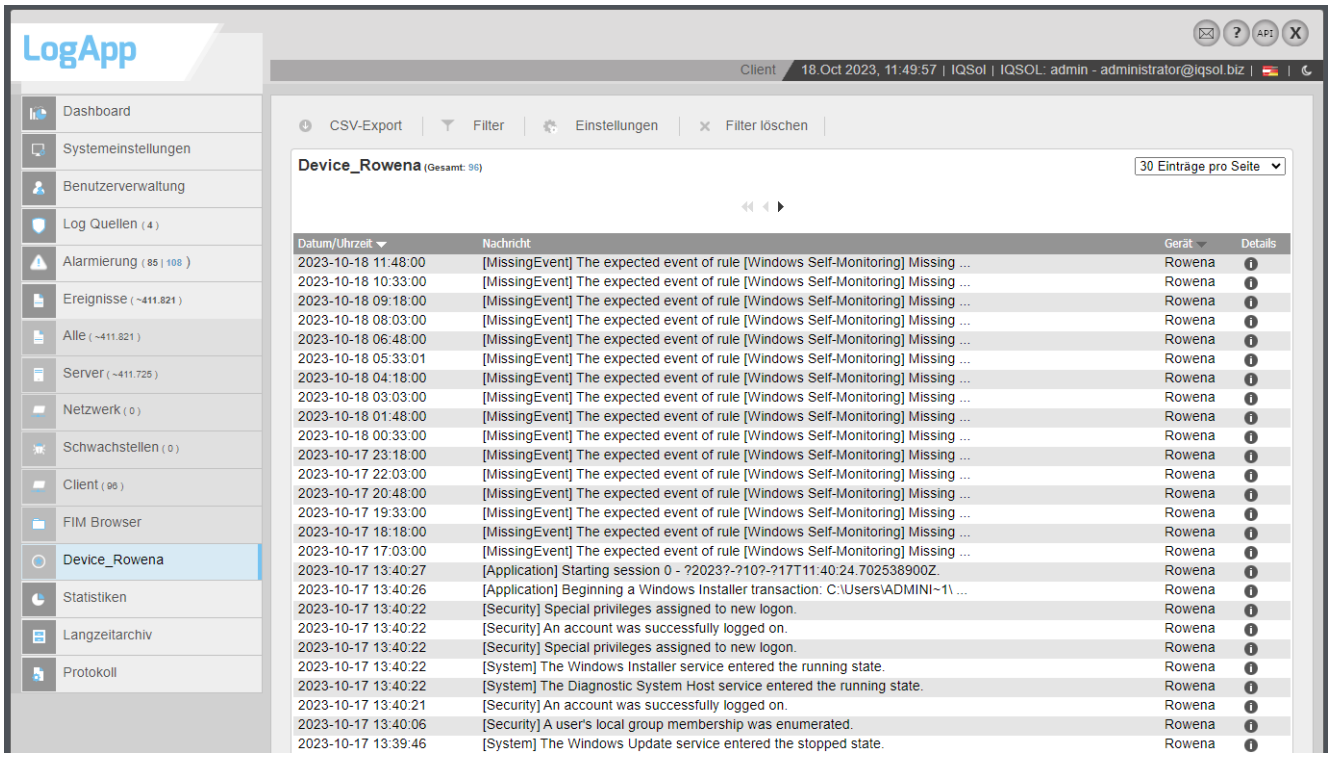

Abbildung 110: Filter als neuer Menüpunkt

7.3 FIM Browser

Unter dem Menüpunkt „FIM Browser“ lassen sich Ergebnisse der File Integrity Scans einsehen und analysieren:

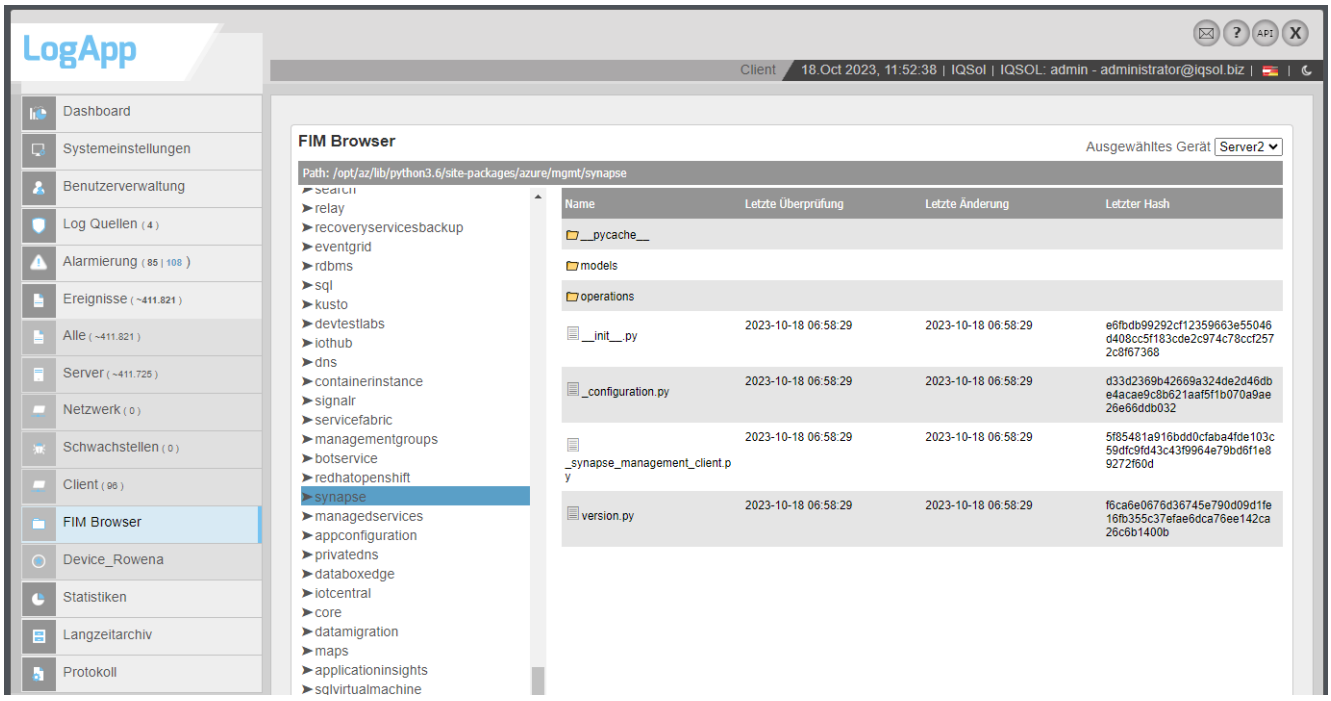

Abbildung 111: FIM Browser

Dazu kann im oberen Bereich ein Gerät ausgewählt werden. Im Navigationsbereich (linke Spalte) werden die gescannten Verzeichnisse angezeigt. Im Detailbereich (rechte Spalte) sind die Verzeichnisse und Dateien des gerade ausgewählten Verzeichnisses sichtbar.

Ein Verzeichnis lässt sich sowohl über einen Klick im Navigationsbereich als auch durch Klick auf den Eintrag des Verzeichnisses im Detailbereich auswählen.

Im Detailbereich sind für gescannte Dateien folgende Einträge zu finden:

- Name des Files
- Zeitstempel der lezten Überprüfung
- Zeitstempel der letzten erfassten Änderung
- Der letzte generierte Hash

7.4 Statistiken

Im Menüpunkt „Statistiken“ können Grafiken und Tabellen erstellt und angezeigt werden. Grafiken und Tabellen können auch als Widget am Dashboard angezeigt werden, sofern die entsprechende Option bei der Erstellung einer Grafik gewählt wird.

Für detaillierte Grafiken kann der IQSol ERS (Enterprise Reporting Server) zum Einsatz kommen.

7.4.1 Grafiken/Tabellen

In der Unterkategorie „Grafiken/Tabellen“ werden die Reports angezeigt. Diese können in Tabs aufgeteilt werden.

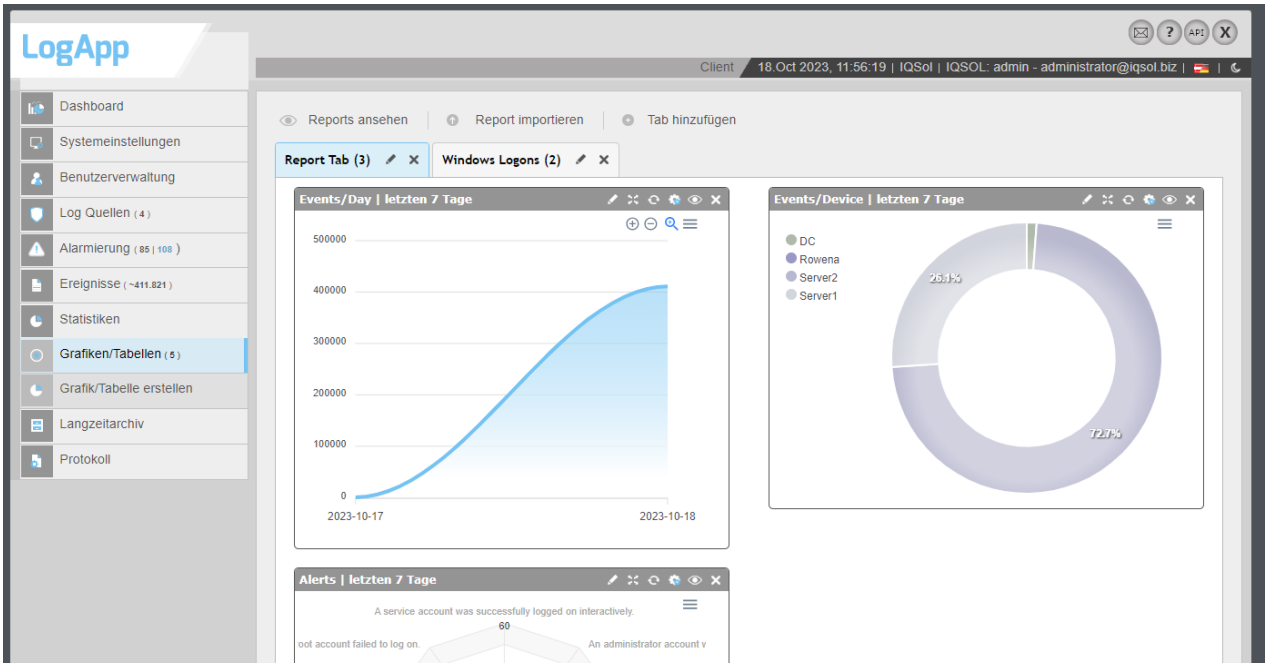

Abbildung 112: Statistikenanzeige

Reports müssen von jedem User hinzugefügt werden. Standardmäßig werden keine Reports angezeigt.

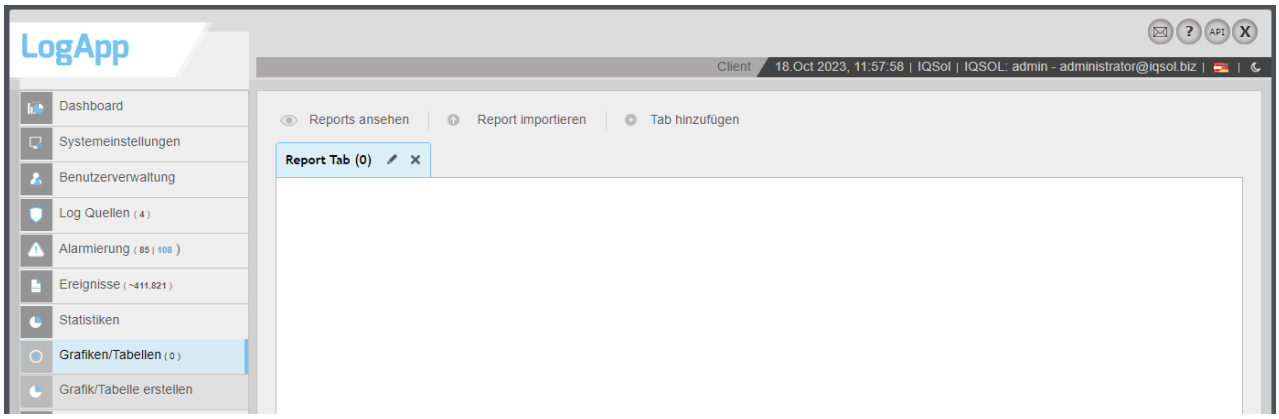

Abbildung 113: Standardanzeige

Mit Klick auf den Button „Reports ansehen“ können Reports hinzugefügt werden. Es sind sechs vordefinierte Reports vorhanden. Diese können ausgewählt und einem Tab zugeordnet werden. Werden zuvor hinzugefügte Reports „versteckt“, so erscheinen diese in dieser Liste. Die Reports werden in den zuvor aktiven Tab angezeigt.

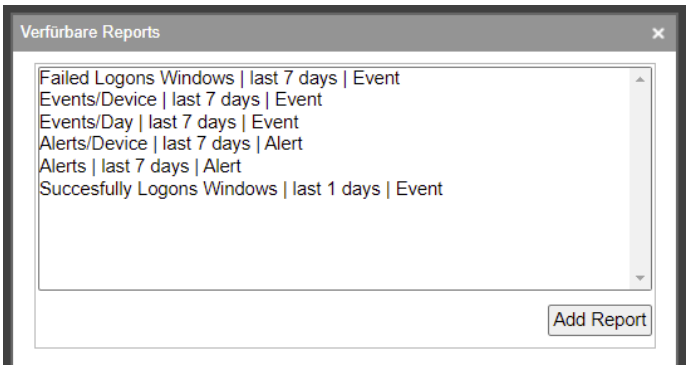

Abbildung 114: Reports hinzufügen

Mit dem „Report importieren“ – Button können exportierte Reports importiert werden. Diese Importe enthalten nur Einstellungen des jeweiligen Reports, es sind keine Daten für die Anzeige des Reports enthalten.

Über den „Add Tab“ – Button können neue Tabs erstellt und Reports hinzugefügt werden.

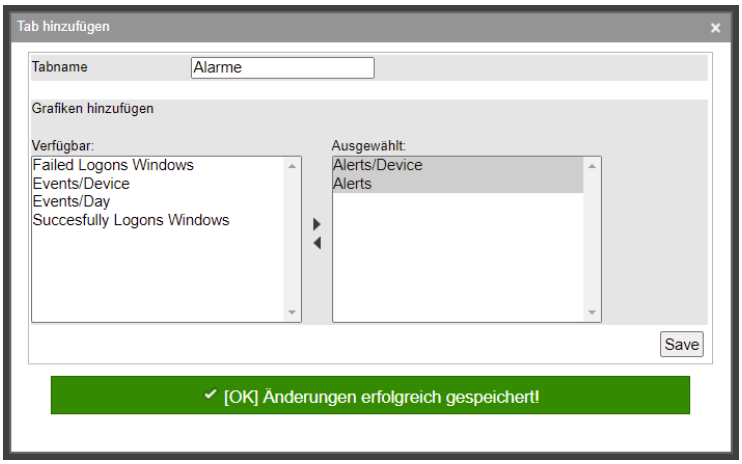

Abbildung 115: neuen Tab erstellen und Reports zuweisen

Neben dem Tab – Namen kann mit einem Klick auf „Edit Tab“ der Name geändert werden. Wird ein Tab nicht mehr benötigt, so kann dieser mit einem Klick auf „Delete/Hide Tab“ gelöscht werden. Enthält dieser Tab noch Reports, so kann ausgewählt werden, ob diese in einen anderen Tab verschoben oder versteckt werden sollen.

Der Standard – Tab, benannt Report Tab, kann nicht gelöscht werden. Es besteht jedoch die Möglichkeit, den Namen zu ändern.

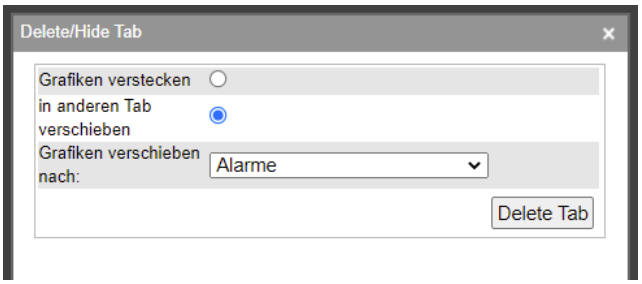

Abbildung 116: Tab löschen

Bei jedem Report können verschiedene Aktionen ausgeführt werden. Folgende Aktionen sind möglich:

Grafiken – Aktionen	
Report bearbeiten	Editieren der Einstellungen (genauere Erklärung siehe nächste Tabelle)
Aktualisieren	Aktualisieren des Reports (Fenstergrößenänderung, aktuelle Daten einsehen, . . .)
Klonen	Der Report wird geklont, alle Einstellungen werden übernommen. Daten für den Report werden nicht dupliziert.
Verstecken	Der Report wird „versteckt“ und kann über den Button „Reports ansehen“ wieder hinzugefügt werden .
Löschen	Report wird gelöscht Ausnahmen: - Standardreports können nur versteckt werden - Reports, welche von einem anderen User erstellt wurden, können nicht gelöscht werden
Aktionen in der Grafik	
Hinein Zoomen	Zoomt in den Report (verfügbar bei Bar und Line Chart)
Hinaus Zoomen	Zoomt aus dem Report (verfügbar bei Bar und Line Chart)
Selektieren	Hier kann nach klick auf das Icon ein bestimmtes Segment im Report ausgewählt werden auf welches danach gezoomt wird. (verfügbar bei Bar und Line Chart)
Download Menü	Download des Report als SVG, PNG oder CSV möglich.
Querlinks	Einige Diagramme haben Querlinks, die direkt zu den ausgewählten Daten führen (z. B. beim Diagramm Events/Tag Doughnut führt die Auswahl eines Kuchenstücks zu den Ereignissen mit dem entsprechenden Filter).

Tabelle 28: Reports - Aktionen

Bei allen Reports, welche Ereignisse als Quelle verwenden, ist es bei bestimmten Grafiken möglich, durch klick auf ein Segment auf die nun gefilterte Ereignissansicht zu springen.

Beispiel:

Der Standard Report Events/Day wird als Säulendiagramm dargestellt.

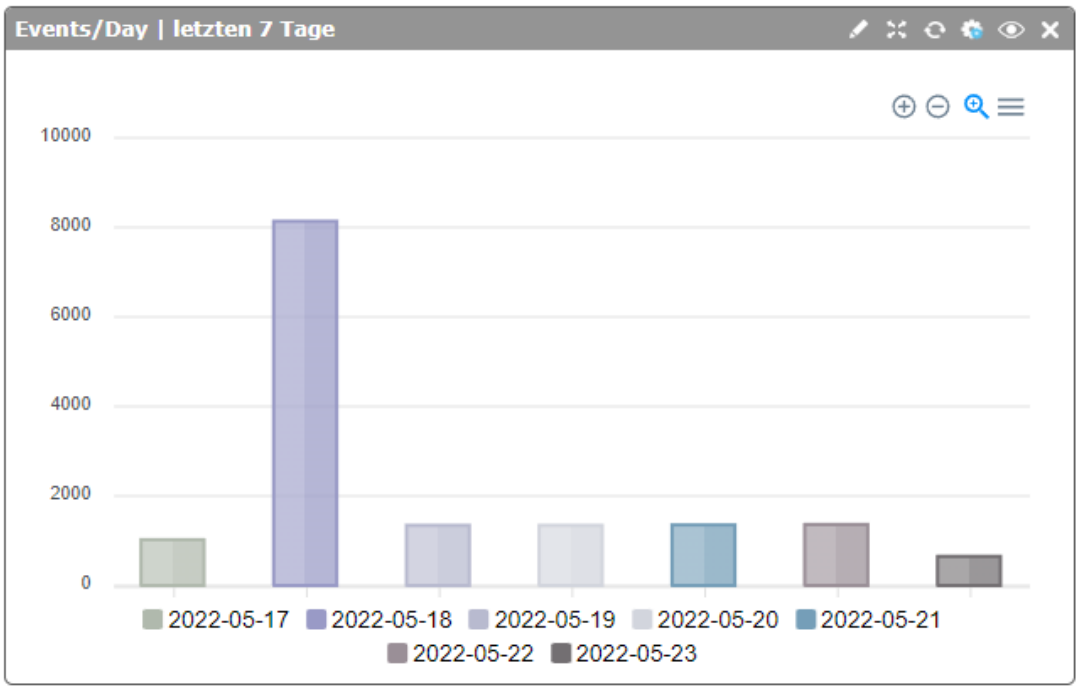

Abbildung 117a: Report – Säulendiagramm

Klickt man nun auf eine beliebige Säule, z.B. auf die Säule mit dem Datum 2022-05-21 so gelangt man zum Menüpunkt „Ereignisse -> Alle“. Hier werden nun alle Ereignisse angezeigt, welche an diesem Tag gelistet wurden.

Auch bei selber erstellten Reports mit unterschiedlichen Filtern kann diese Funktion genutzt werden.

Dies funktioniert mit Säulen, Balken, Kreis und Doughnut Diagrammen.

Bei einem Klick auf „Report bearbeiten“ können folgende Einstellungen vorgenommen werden:

Reports bearbeiten	
Name	Änderung des Namens
Grafik	Auswahl der Report– Art (Balken, Säulen, Tabelle, . . .)
Limit	Anzahl der verschiedenen Datensätze die im Report angezeigt werden sollen
Zeit	Auswahl der Zeitspanne
Ordnen nach	Auswahl, ob nach der Anzahl der Events oder des Labels sortiert werden soll
Richtung	Aufsteigende oder Absteigende Sortierung auswählen
Tab zuordnen	Report einem anderen Tab zuweisen
Mit allen Benutzergruppen teilen	Der Report kann von allen Benutzergruppen hinzugefügt werden .
Mit ausgewählten Benutzer Gruppen teilen	Der Report kann von ausgewählten Benutzergruppen hinzugefügt werden.

Tabelle 29: Report - Einstellungen

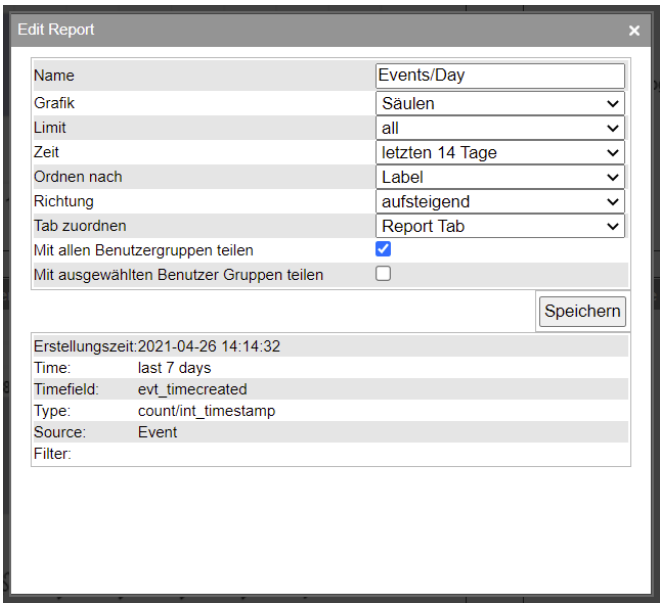

Abbildung 118: Report - Einstellungen

7.4.2 Grafik/Tabelle erstellen

Hier können Grafiken und Tabellen erstellt werden.

Wird ein neuer Report erstellt, so werden ab diesem Zeitpunkt Events (oder Alarme) aufgezeichnet. Ein Historischer Report, zur Anzeige von vergangenen Events, ist nicht möglich.

Folgende Auswahlmöglichkeiten stehen bei einer Neuerstellung zur Verfügung:

Grafik/Tabelle erstellen	
Name	Name des Reports
Quelle	Auswahl, ob der Report Events oder Alarme erfassen soll
Filter	Auswahl einer Filterung Die meisten Filteroptionen werden als Text (String) eingegeben und mittels RegEx generiert (ident mit der Filterung bei Ereignissen). Vordefinierte Optionen können in folgenden Unterkategorien ausgewählt werden: - Events -> Log-> Geräte - Alarme-> Priorität - Alarme-> Status - Alarme-> Verantwortlicher - Alarme -> Geräte
Report	Hier ist folgendes auszuwählen:
Typ	Auswahl des Typs (EventID, Timestamp,)
Zeit	Definiert einen Zeitraum, für die Ansicht des Reports
Diagramm oder Tabelle	Auswahl, ob es eine Tabelle oder ein Diagramm sein soll
Diagramm	Hier wird ausgewählt, welche Art von Report erstellt werden soll (Balken, Säulen, . . .)
Benutzergruppeneinstellungen	Hier kann der erstellte Report mit allen, oder mit ausgewählten Benutzergruppen geteilt werden. Die Reports können somit von allen User, die Mitglieder dieser Gruppen sind, hinzugefügt werden

Tabelle 30: Grafik/Tabelle erstellen

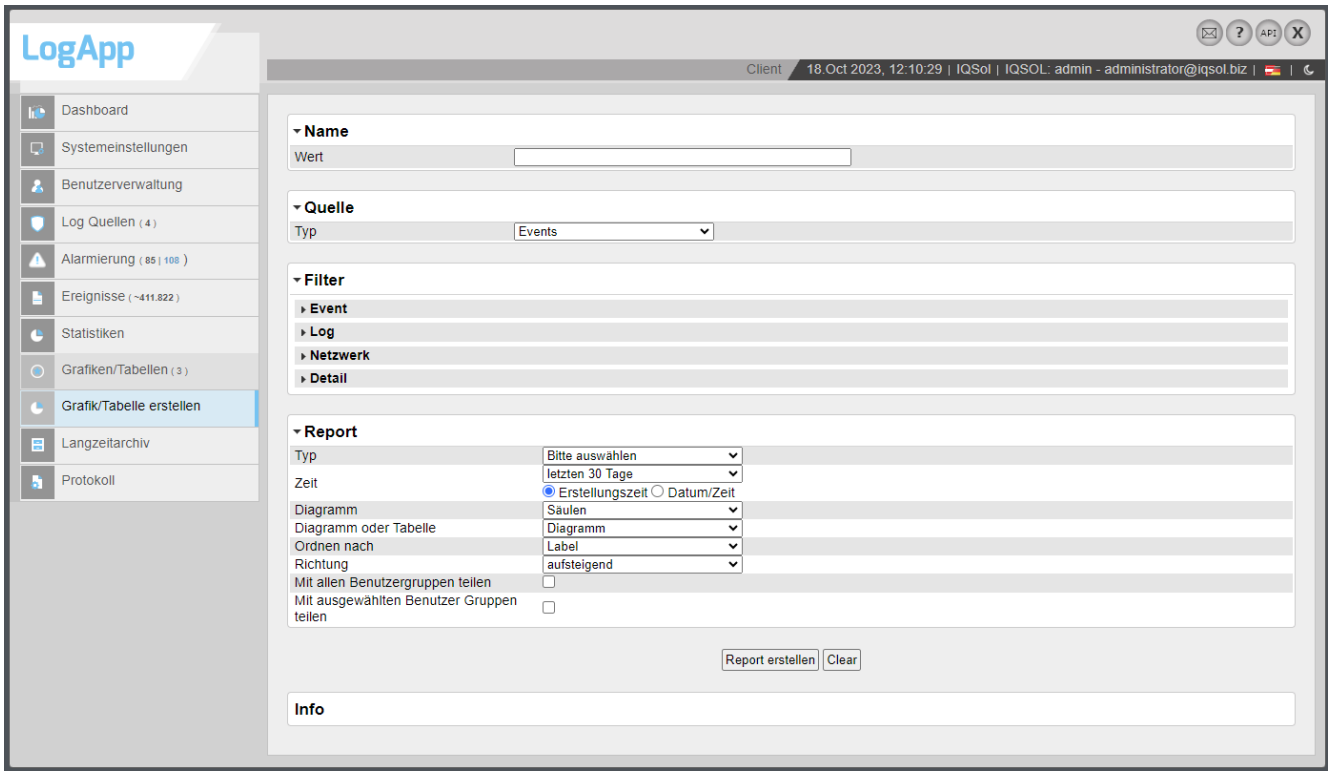

Abbildung 119: Report - Einstellungen

7.5 Langzeitarchiv

Wird der Export aktiviert so werden jede Nacht alle Ereignisse des letzten Tages exportiert und als signierte Archiv-Datei gespeichert (optional verschlüsselt). Entsprechend der Konfiguration wird die Datei lokal auf der LogApp oder auf einer externen SMB-Freigabe abgelegt.

7.5.1 Exporte

Unter „Exporte“ werden die erstellten Archivdateien angezeigt. In der Sektion „Lokale Exporte“ werden die Archive auf der LogApp angezeigt. Mit den Buttons in der Liste können die Archive auf die externe Freigabe kopiert oder verschoben werden bzw. auf Archive auf LogApp wiederhergestellt oder gelöscht werden.

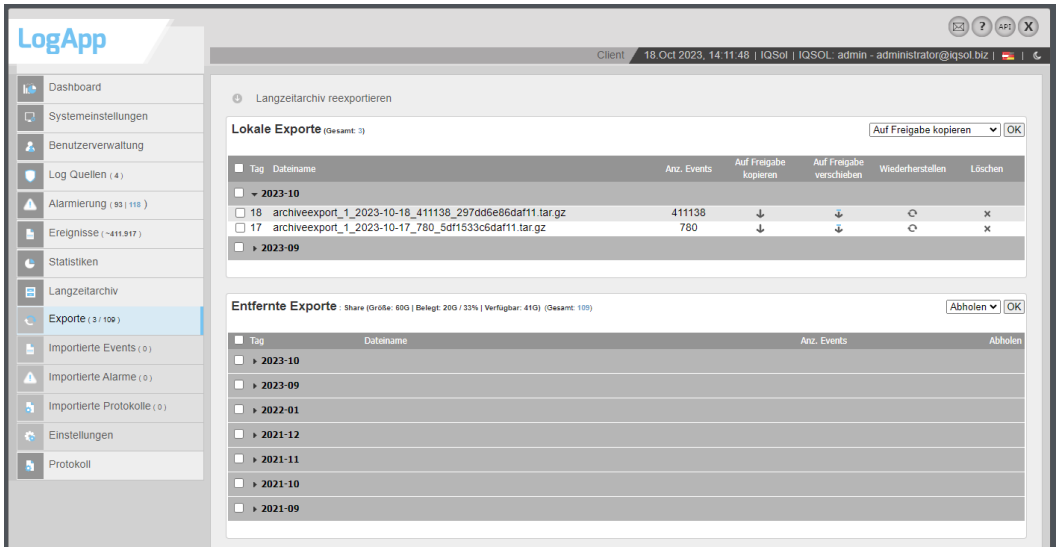

Abbildung 120: Langzeitarchiv

In der Sektion „Entfernte Exporte“ werden die Archive auf der eingestellten Freigabe angezeigt. Mit dem „Abholen“-Button können die Archive auf die LogApp kopiert werden. Anschließend können die Archive importiert werden. Archive können manuell von der externen Freigabe entfernt und im Bedarfsfall wieder dort abgelegt werden.

Bei der Wiederherstellung von Archiven ist es möglich, ein ganzes Archiv (ganzer Tag) oder eine einzelne Stunde eines Archives zu reimportieren (empfehlenswert bei sehr großen Archiven, um die Importdauer zu reduzieren). Es können auch mehrere Stunden ausgewählt werden mit gedrückt gehaltener Strg-Taste + Linksklick.

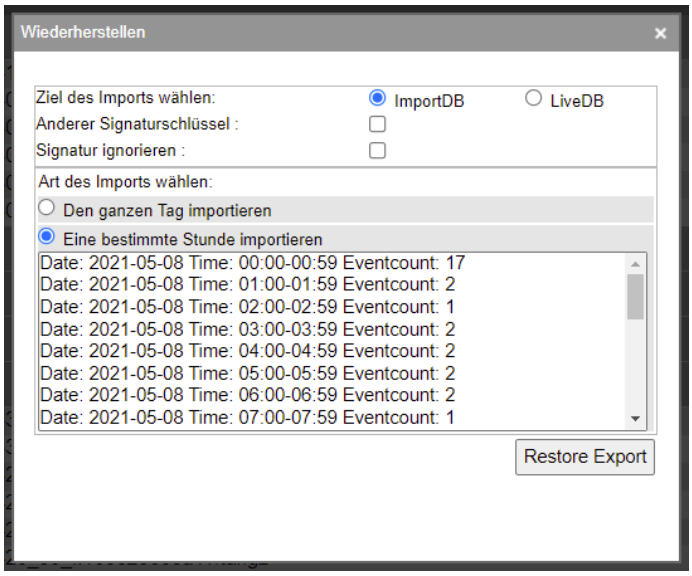

Abbildung 121: Langzeitarchiv Wiederherstellungsoptionen

Als weitere Option kann das Ziel des Imports ausgewählt werden. Wird eine LogApp aus einem Backup wiederhergestellt so können hier die im Backup nicht enthaltenen Ereignisse selektiv wieder eingespielt werden. Hierzu muss das Ziel „LiveDB“ ausgewählt werden. Bei einem Import in die „LiveDB“ werden nur die Events importiert (Kein Import der Alarme oder Protokolle). Wird das Ziel „ImportDB“ ausgewählt so befinden sich die eingespielten Ereignisse und deren Alarme in den Jeweiligen Importansichten (z.B. Importierte Events).

Sollen Ereignisse einer anderen LogApp eingespielt werden, so kann ein anderer Signaturschlüssel eingespielt werden. Hierzu muss die entsprechende Option ausgewählt werden und das Archiv mit den Schlüsseln ausgewählt werden. Diese lassen sich von der Original LogApp im „Backup/Restore“-Menü exportieren.

Wird das Ziel „ImportDB“ ausgewählt so ist es möglich die Signaturprüfung zu überspringen.

Bulk Operationen:

Als Bulkoperationen stehen folgende Möglichkeiten zur Verfügung:

- Auf Freigabe kopieren
- Auf Freigabe verschieben
- Löschen
- Neu verschlüsseln

Langzeitarchive neu verschlüsseln

Wird eine LogApp neu installiert oder will man Archive von anderen LogApps in einer LogApp verwalten, oder sollte sich der Schlüssel aus einem anderen Grund verändern, so ist es möglich, ein Archiv neu zu verschlüsseln. Hierzu wird der alte Schlüssel verlangt (public.pem). Dieser kann in einem Uploaddialog hochgeladen werden.

Mit diesem wird das Archiv entschlüsselt, anschließend wird es mit dem aktuellen PrivateKey verschlüsselt.

7.5.2 Importierte Events

Unter dem Menüpunkt „Importierte Events“ können wiederhergestellte Ereignisse aus Archivdateien eingesehen werden. Mit dem Button „Importe löschen“ können die importierten Ereignisse wieder aus der Datenbank gelöscht werden.

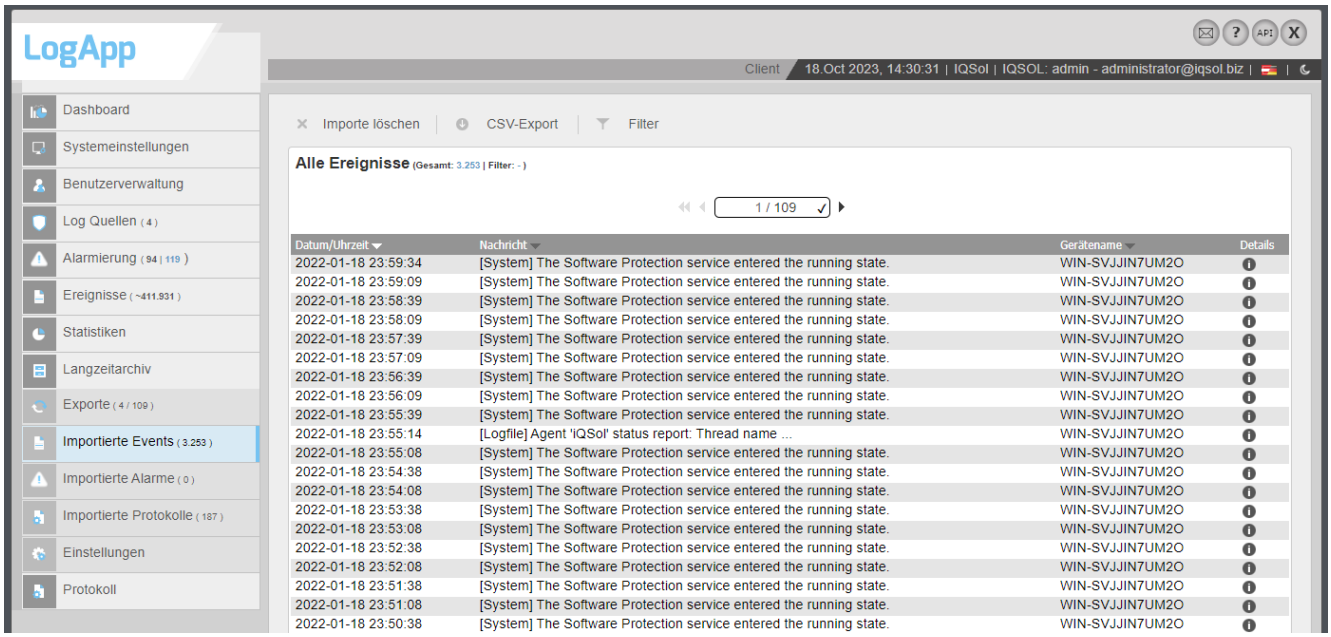

Abbildung 122: Importierte Events

7.5.3 Importierte Alarme

Neben den Menüpunkt „Importierte Events“ können ebenso „Importierte Alarme“ mit dem entsprechenden Ereignis, die den einzelnen Alarm getriggert haben, betrachtet werden. Ebenso besteht die Möglichkeit, die Alarme zu filtern und die zugewiesenen Alarme einzusehen.

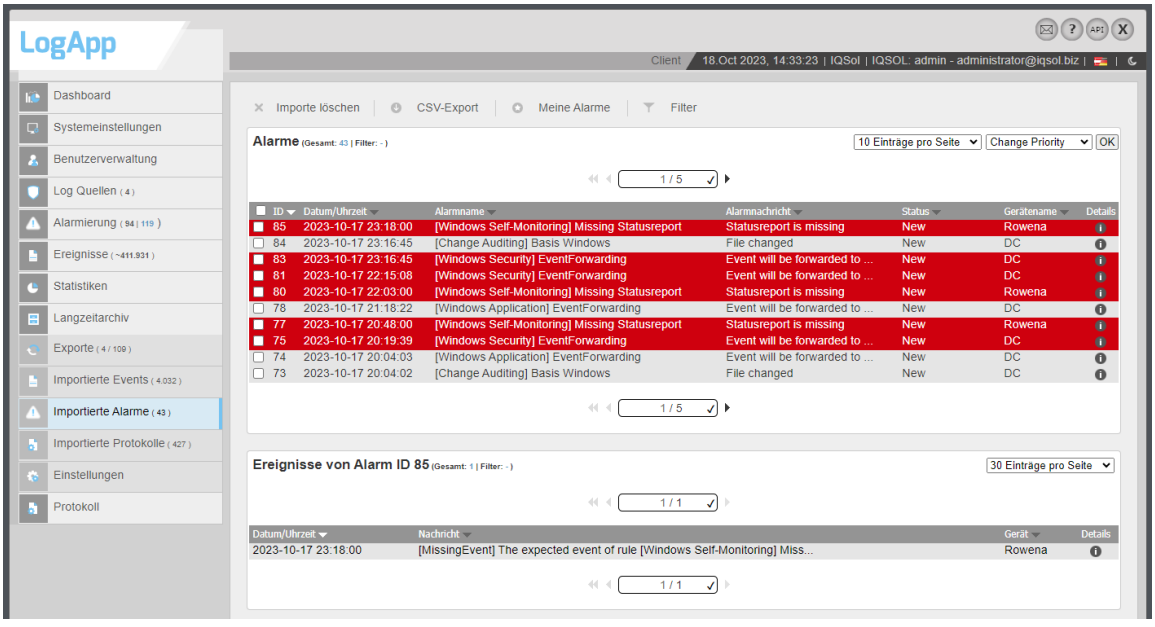

Abbildung 123: Importierte Alarme

7.5.4 Importierte Protokolle

Unter dem Menüpunkt „Importierte Protokolle“ können Ereignisse betrachtet werden, die das interne Protokoll der LogApp darstellt.

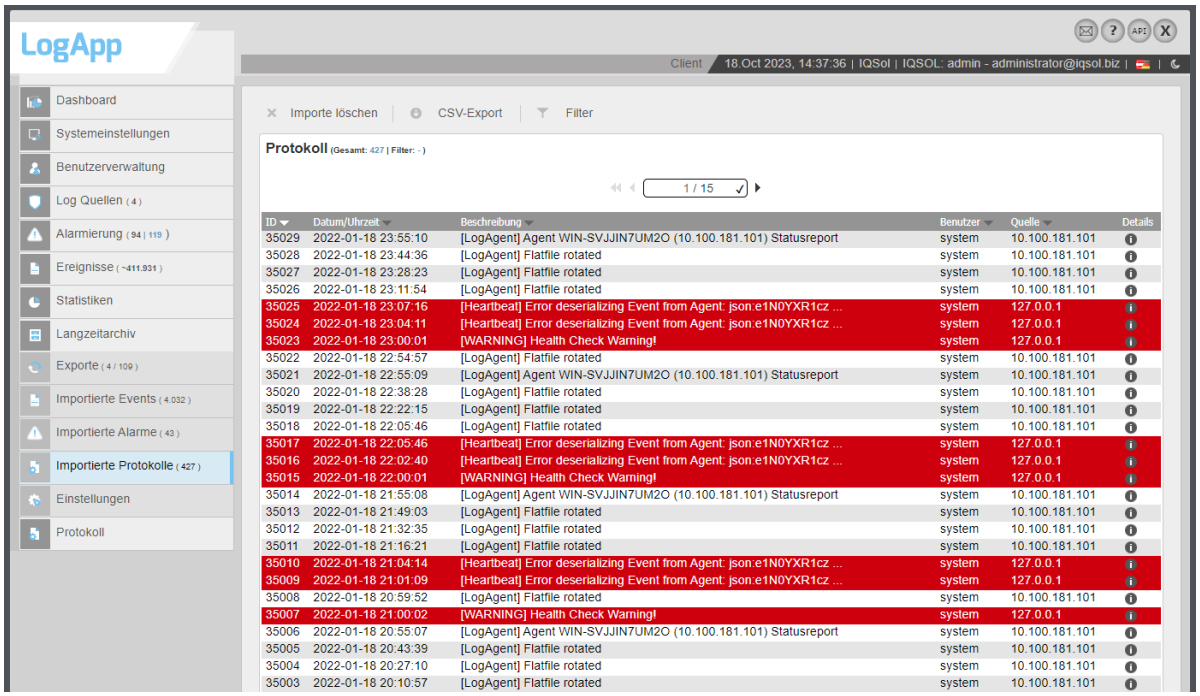

Abbildung 124: Importierte Protokolle

7.5.5 Einstellungen

In den Einstellungen für das Langzeitarchiv können externe Speicherorte wie Windows Shares (SMB/CIFS), S3 Buckets (AWS), Azure Blobs oder SSHFS angegeben werden. Wenn keine Einstellungen getroffen werden, werden die Archive lokal abgelegt. Bitte beachten Sie, dass je nach Datenmenge und verfügbarem Speicherplatz der Festplattenplatz der LogApp schnell erschöpft sein kann.

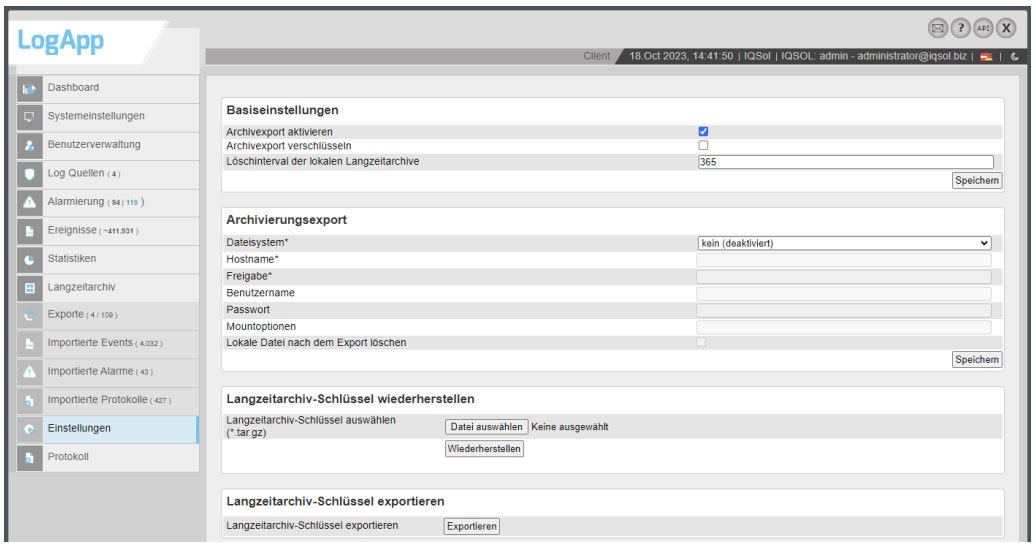

Abbildung 125: Importierte Protokolle

Option	Beschreibung
Basiseinstellungen	
Archivexport aktivieren	Das Setzen dieser Option aktiviert die Erzeugung von Archiven.
Archivexport verschlüsseln	Das Setzen dieser Option aktiviert die Verschlüsselung der erzeugten Archive.
Löschintervall der lokalen Langzeitarchive	Wert, nach wie vielen Tagen Archivfiles lokal auf der LogApp gelöscht werden.
Archivierungsexport	
Dateisystem	Auswahl des Dateisystems für das Langzeitarchiv, z.B. SMB/CIFS-Freigabe, S3 Bucket (AWS), Azure Blob, SSHFS oder lokal
Hostname	FQDN (Fully Qualified Domain Name) oder IP des File Servers
Freigabe	Freigabename auf dem File Server
Benutzername	Benutzername für die Authentifizierung
Passwort	Passwort für die Authentifizierung
Datenspeicher (S3 AWS)	Der S3 Bucket, in dem die Daten für das Langzeitarchiv gespeichert werden.
Zugriffsschlüssel-ID (S3 AWS)	AccessKeyId für den S3 Bucket (AWS). Sie wird verwendet, um auf die AWS-Ressourcen zuzugreifen und die Authentifizierung bei der Nutzung von AWS-Diensten sicherzustellen.
Geheimer Zugriffsschlüssel (S3 AWS)	SecretAccessKey für den S3 Bucket (AWS). Dieser Schlüssel wird zusammen mit der Zugriffsschlüssel-ID verwendet, um die Authentifizierung und den Zugriff auf AWS-Dienste zu gewährleisten.
Container (Azure)	Der Container bezieht sich auf die Azure Blob Storage. In Azure Storage ist ein Container eine logische Gruppierung von Blobs, die verwendet wird, um Daten zu organisieren und zu verwalten. Jeder Container kann mehrere Blobs enthalten, und der Container-Name muss innerhalb des Azure Storage-Kontos eindeutig sein.
Kontoname (Azure)	Der Kontoname bezieht sich auf den Namen des Azure Storage-Kontos. Jedes Azure Storage-Konto hat einen eindeutigen Namen, der im Azure-Portal verwendet wird, um auf die Ressourcen des Kontos zuzugreifen. Der Kontoname muss global eindeutig sein und wird verwendet, um auf die Blob-Daten zuzugreifen und diese zu verwalten.
Kontoschlüssel (Azure)	Der Kontoschlüssel ist ein geheim gehaltenes Passwort, das mit dem Azure Storage-Konto verknüpft ist.
Mountoptionen	Optionen, welche dem Linux Mount Befehl mitgegeben werden können, z.B. sec=ntlmv2i, DOMAIN='example, vers=2.0'. Details entnehmen Sie dazu den mount man pages. Zum Testen kann

	folgender Mount-Befehl verwendet werden (mit oben genannten Optionen): `sudo USER='YYY' PASSWD='XXX' mount -o sec=ntlmv2i,DOMAIN='ZZZ',uid=www-data,gid=www-data -t cifs //192.168.205.131/laa/ /archive/2/ 2>&1`
Lokale Datei nach dem Export löschen	Aktivieren, um das Archiv nur auf dem externen Share abzulegen (empfohlen)
Langzeitarchiv-Schlüssel wiederherstellen	
Langzeitarchiv-Schlüssel auswählen (*.tar.gz)	Ein zuvor exportierter Schlüssel kann ausgewählt und wiederhergestellt werden.
Langzeitarchiv-Schlüssel exportieren	
Langzeitarchiv-Schlüssel exportieren	Der Langzeitarchiv-Schlüssel der LogApp kann exportiert werden.

Tabelle 31: Einstellungen für das Langzeitarchiv

7.6 Protokoll

Unter dem Menüpunkt „Protokoll“ werden Systemereignisse und sicherheitsrelevante Vorfälle die LogApp selbst betreffend aufgezeichnet.

Das Protokoll ist in folgende Kategorien unterteilt:

Modus	Beschreibung
System	Änderungen in Systemeinstellungen und Systemereignisse
Benutzer	Änderungen in der Benutzerverwaltung, Anmeldevorgänge, Protokolle der Eventanzeige
Geräte	Ereignisse betreffend LogAgents und Netzwerkgeräten
Alarme	Änderungen an den Alarmierungseinstellungen
API	Statusmeldungen der REST API, wie auhtentifizierungsversuche, etc.

Tabelle 32: Protokollkategorien

Protokolleinträge werden jeweils mit Daten/Uhrzeit, einer Beschreibung, einem Benutzer und einer Quell-IP angezeigt. Der Benutzer ist entweder der angemeldete Benutzer mit seiner Client-IP oder der Benutzer „system“ mit der IP 127.0.0.1. Mit dem „Details“-Button können weitere Details zu den Ereignissen eingesehen werden. Der „Filter“-Button im oberen Bereich der Seite ermöglicht das Suchen in den Protokolleinträgen. ID, Datum/Uhrzeit, Beschreibung, Benutzer und Quell-IP können beliebig eingeschränkt werden, um nach bestimmten Ereignissen zu suchen.

Anhang

Deaktivieren der Benutzerkontensteuerung unter Windows

Auf Windows Betriebssystemen ohne Domänenmitgliedschaft kann die Benutzerkontensteuerung in der Lokalen Sicherheitsrichtlinie deaktiviert werden. Dabei sollte die Policy „User Account Control: Behaviour of the elevation prompt for administrators in Admin Approval Mode "auf den Wert „Elevate without prompting" gestellt werden.

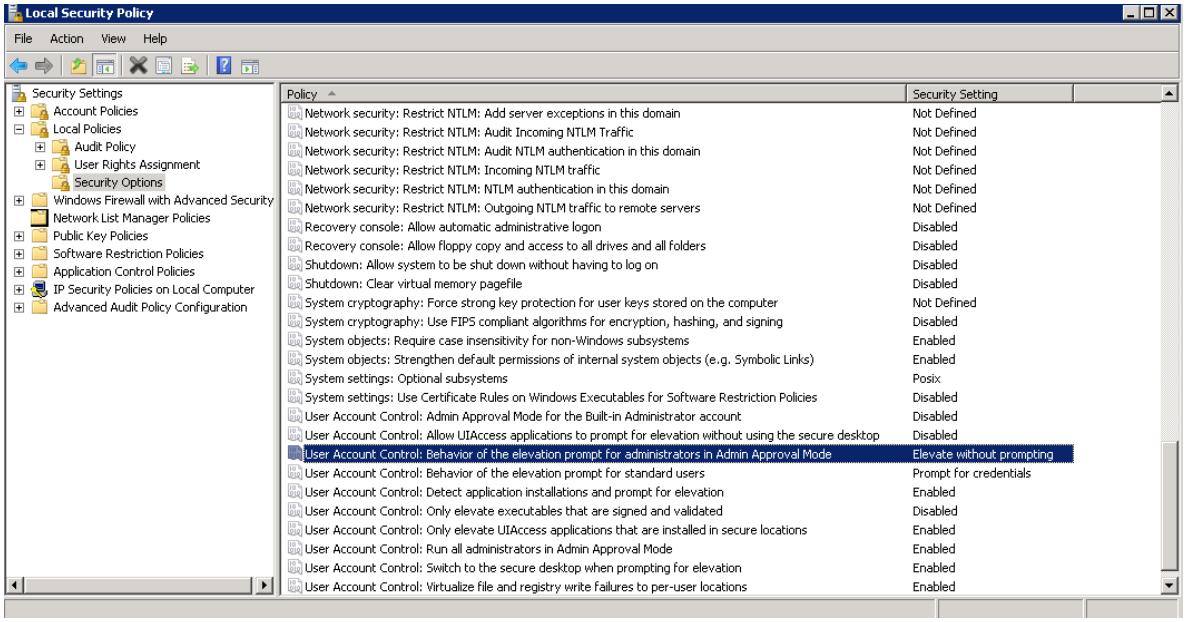

Abbildung 126: Lokale Sicherheitsrichtlinie

Bei Computern mit Domänenmitgliedschaft sollte die Einstellung in einer Gruppenrichtlinie definiert werden, die in der folgenden Abbildung dargestellt ist.

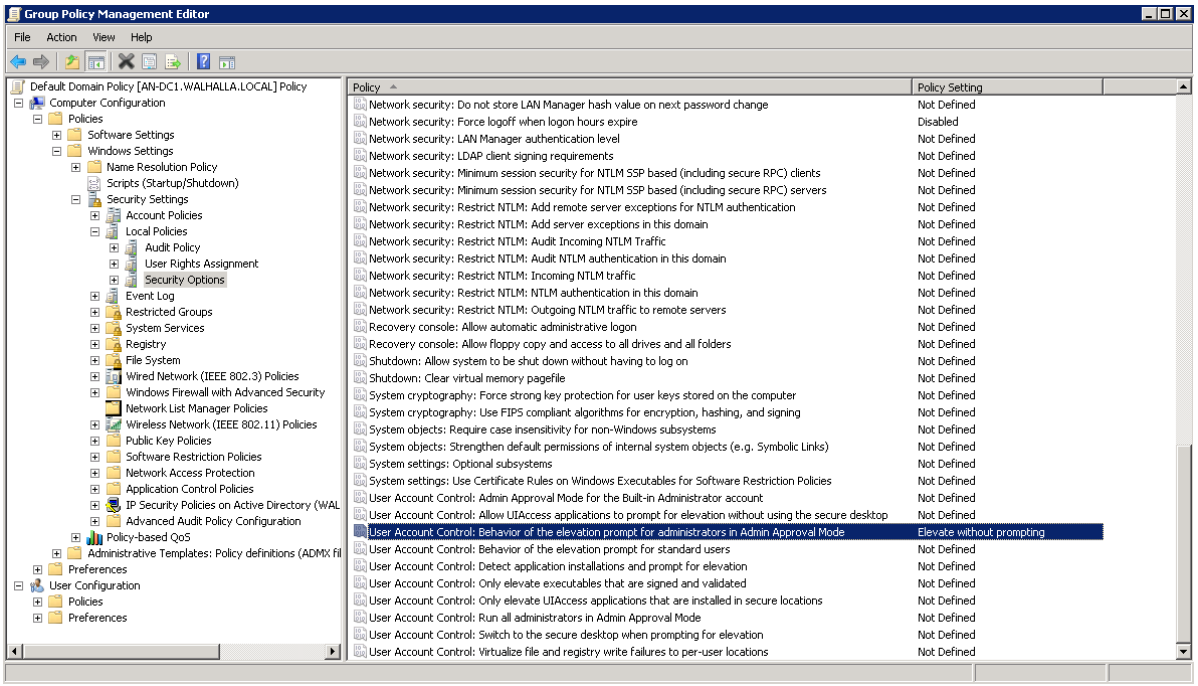

Abbildung 127: Gruppenrichtlinie

Konfiguration für Logfiles und Syslog

Zeitformat

Das Zeitformat gibt an, wie Datum und Uhrzeit in den Logs aufgebaut sind. Diese Angabe ist nötig, um den Zeitstempel, welcher im Feld evt_timecreated gespeichert ist, richtig verarbeiten und normalisieren zu können.

Die in der folgenden Tabelle (Quelle: http://msdn.microsoft.com/de-de/library/8kb3ddd4%28v=vs.80%29.aspx) angeführten Formatbezeichner können verwendet werden:

Formatbezeichner	Beschreibung
d	Stellt den Tag eines Monats als Zahl von 1 bis 31 dar. Einstellige Tage werden ohne führende Null formatiert.
dd	Stellt den Tag eines Monats als Zahl von 01 bis 31 dar. Einstellige Tage werden mit einer führenden Null formatiert.
ddd	Stellt den abgekürzten Namen des Wochentags dar.
dddd	Stellt den vollständigen Namen des Wochentags dar.
h	Stellt die Stunde als Zahl von 1 bis 12 dar. Die Stunde wird dabei im 12-Stunden-Format dargestellt, bei dem die ganzen Stunden ab Mitternacht oder 12 Uhr mittags gezählt werden. Infolgedessen lässt sich eine Stunde nach Mitternacht nicht von derselben Stunde nach 12 Uhr mittags unterscheiden. Die Stunde wird nicht gerundet. Einstellige Stunden werden ohne führende Null formatiert.
hh	Stellt die Stunde als Zahl von 01 bis 12 dar. Die Stunde wird dabei im 12-Stunden-Format dargestellt, bei dem die ganzen Stunden ab Mitternacht oder 12 Uhr mittags gezählt werden. Infolgedessen lässt sich eine Stunde nach Mitternacht nicht von derselben Stunde nach 12 Uhr mittags unterscheiden. Die Stunde wird nicht gerundet. Einstellige Stunden werden mit einer führenden Null formatiert.
H	Stellt die Stunde als Zahl von 0 bis 23 dar. Die Stunde wird dabei im nullbasierten 24-Stunden-Format dargestellt, bei dem die Stunden ab Mitternacht gezählt werden. Einstellige Stunden werden ohne führende Null formatiert.
HH	Stellt die Stunde als Zahl von 00 bis 23 dar. Die Stunde wird dabei im nullbasierten 24-Stunden-Format dargestellt, bei dem die Stunden ab Mitternacht gezählt werden. Einstellige Stunden werden mit einer führenden Null formatiert.
m	Stellt die Minute als Zahl von 0 bis 59 dar. Die Minute stellt die seit der letzten Stunde vergangenen ganzen Minuten dar. Einstellige Minuten werden ohne führende Null formatiert.
mm	Stellt die Minute als Zahl von 00 bis 59 dar. Die Minute stellt die seit der letzten Stunde vergangenen ganzen Minuten dar. Einstellige Minuten werden mit einer führenden Null formatiert.
M	Stellt den Monat als Zahl von 1 bis 12 dar. Einstellige Monate werden ohne führende Null formatiert.
MM	Stellt den Monat als Zahl von 01 bis 12 dar. Einstellige Monate werden mit einer führenden Null formatiert.
MMM	Stellt den abgekürzten Namen des Monats dar.
MMMM	Stellt den vollständigen Namen des Monats dar.
s	Stellt die Sekunden als Zahl von 0 bis 59 dar. Einstellige Sekunden werden ohne führende Null formatiert.
ss	Stellt die Sekunden als Zahl von 00 bis 59 dar. Einstellige Sekunden werden mit einer führenden Null formatiert.

y	Stellt das Jahr als eine höchstens zweistellige Zahl dar. Falls das Jahr mehr als zwei Ziffern umfasst, werden im Ergebnis nur die beiden niedrigwertigen Ziffern angezeigt. Umfasst das Jahr weniger als zwei Ziffern, wird die Zahl ohne führende Null formatiert.
yy	Stellt das Jahr als zweistellige Zahl dar. Falls das Jahr mehr als zwei Ziffern umfasst, werden im Ergebnis nur die beiden niedrigwertigen Ziffern angezeigt. Umfasst das Jahr weniger als zwei Ziffern, wird die Zahl mit führenden Nullen auf eine zweistellige Jahresangabe aufgefüllt.
yyy	Stellt das Jahr als dreistellige Zahl dar. Falls das Jahr mehr als drei Ziffern umfasst, werden im Ergebnis nur die drei niedrigwertigen Ziffern angezeigt. Umfasst das Jahr weniger als drei Ziffern, wird die Zahl mit führenden Nullen auf eine dreistellige Jahresangabe aufgefüllt.
yyyy	Stellt das Jahr als vierstellige Zahl dar. Falls das Jahr mehr als vier Ziffern umfasst, werden im Ergebnis nur die vier niedrigwertigen Ziffern angezeigt. Umfasst das Jahr weniger als vier Ziffern, wird die Zahl mit führenden Nullen auf eine vierstellige Jahresangabe aufgefüllt.
%s	Stellt die Sekunden seit Epoch (1. Januar 1970, 00:00 Uhr UTC) dar und entspricht dem Unixtimestamp.

Wenn das angegebene Zeitformat nicht verarbeitet werden kann, oder kein Zeitformat angegeben wird, wird das Ereignis mit der aktuellen Uhrzeit des Agents gespeichert.

Parsemaps

Eine Parsemap ist eine XML Struktur, welche definiert wie aus einem Log-Eintrag ein Ereignis generiert wird.

Hierzu wird eine XML Struktur verwendet, welche ein <maps> rootelement besitzt und sich aus beliebig vielen einzelnen Map Tags zusammensetzt. Eine Beispielhafte Struktur wäre:

```
<maps>
	<map>
		<identifier>(.*)</identifier>
		<blacklist>
			<blacklist_identifier>RegEx</blacklist_identifier>
			<blacklist_identifier>RegEx</blacklist_identifier>
		</blacklist>
		<regex>
			<attribute save="true" name="Name1">RegEx</attribute>
			<attribute save="true" name="Name2">RegEx</attribute>
			...
		</regex>
		<staticinfo>
			<attribute save="true" name="Name3">StaticValue</attribute>
			<attribute save="true" name="Name4">StaticValue</attribute>
			...
		</staticinfo>
		<labelmapid>ID</labelmapid>
	</map>
	...
</maps>
```

Elemente einer Parsemap

Eine Parsemap besteht im Wesentlichen aus 8 verschiedenen Blöcken:

- Identifier
- Settings
- Timeformat
- Blacklist
- Regex
- Staticinfo
- Labelmapid
- Seperator (nur bei CSV Modus nötigt)

Im Folgenden werden die einzelnen Blöcke genauer erläutert.

Identifier

Jedes Map Element muss genau einen Identifier haben. Ein Identifier ist ein XML Element mit dem Tagnamen identifier und einer Regex als Value. Beispiel:

```
<identifier>(.*)</identifier>
```

Ein Identifier dient wie der Name schon sagt dem identifizieren der richtigen Map. Hierbei iteriert der LogAgent bei jedem zu verarbeitenden LogEintrag durch alle Map Elemente von oben nach unten, die erste map mit einem übereinstimmenden Identifier wird zur Verarbeitung des Logeintrages herangezogen. Sollte kein Identifier übereinstimmen wird der LogEintrag verworfen.

Sollte der ParsingModus XML sein, so wird überprüft, ob die RegEx auf einen Tag Namen zutrifft. Ist dies der Fall, so wird dieser Tag von der Parsemap verwendet um ein Event zu generieren.

Für die Logzeile

```
date=2014-10-01 time=19:20:24 devname=FG50BH3G09600012 device_id=FG50BH3G09600012
log_id=0104032001 type=event subtype=admin pri=information vd=root user="admin"
ui=http(192.168.1.110) action=login status=success reason=none
profile="super_admin" msg="Administrator admin logged in successfully from
http(192.168.1.110)"
```

wäre `<identifier>(\stype=(event)\s)subtype=(admin)</identifier>` ein passendes identifier-Element.

Settings

Mit dem Settingselement lassen sich Einstellung sowohl für das betroffene Mapelement, als auch global festlegen. Für globale Einstellungen muss das Settingselement außerhalb der Mapelemente, am besten gleich nach dem Mapselement, platziert werden.

Globale Einstellungen werden von den Einstellungen in einer Map (sofern spezifiziert) überschrieben.

Sowohl globale Settings, als auch Settings per Map sind optional.

Folgende Einstellungen sind möglich:

- Discardeventsfornotmatchingmap:
  Mit diesem Setting ist es möglich zu spezifizieren ob Ereignisse, welch nicht beim Abarbeiten der Parsemap matchen zu sammeln, zu zählen oder zu verwerfen. Mögliche Werte sind:
  - Yes (default): Events werden verworfen
  - No: Ereignisse werden gesammelt und als Warnung ausgegeben
  - Count: Ereignisse werden gezählt und in einer eigenen Meldung ausgegeben
- Countnotmatchingidentifiers:
  Mit diesem Setting lässt sich festlegen, ob die Logeinträge für welche kein passender Identifier existiert gezählt werden. Mögliche Werte sind yes und no (default)
- Countdiscardedeventsblacklist:
  Dieses Setting definiert ob Ereignisse, welche aufgrund der Blacklist ausgefiltert werden, gezählt werden sollen. Mögliche Werte sind yes und no(default)

Beispiel:

```
<maps>
  <settings>
    <discardeventsfornotmatchingmap>count</discardeventsfornotmatchingmap>
    <countnotmatchingidentifiers>yes</countnotmatchingidentifiers
    <countdiscardedeventsblacklist>yes</countdiscardedeventsblacklist>
    </settings>
  <map>
    <settings>
      <discardeventsfornotmatchingmap>count</discardeventsfornotmatchingmap>
      <countnotmatchingidentifiers>yes</countnotmatchingidentifiers
      <countdiscardedeventsblacklist>yes</countdiscardedeventsblacklist>
      </settings>
.
    .
```

Timeformat

Zusätzlich zum globalen Zeitformat, welches außerhalb der Parsemap in der Konfigurationsgruppe definiert wird, lässt sich auf für jedes Mapelement ein Zeitformat angeben mit dem das Attribut evt_timecreated in einen gültigen Zeitstempel umgewandelt wird. Dieses Element ist optional.

Beispiel:

```
<maps>
      <map>
         <datetimeformat>dd.MM.yyyy HH:mm:ss</datetimeformat>
<identifier> …
.
.
```

Blacklist

Das Blacklistelement ist eine Liste von Subelementen mit den Namen blacklistidentifier.

Mithilfe dieser Identifier lassen sich Elemente, welche zwar mit dem Identifier übereinstimmen, aber trotzdem unerwünscht sind, gezielt ausfiltern.

Die Subelemente blacklistidentifier haben hierbei als Wert eine RegEx.

Sollte eine Parsemap einen übereinstimmenden Identifier haben, wird falls vorhanden überprüft ob ein blaklistidentifier Element mit dem Logeintrag übereinstimmt. Trifft dies zu, so wird dieses Event verworfen.

Beispiel:

```
<maps>
  <map>
    <identifier>.*</identifier>
    <blacklist>
      <blacklistidentifier>DEBUG</blacklistidentifier>
    </blacklist>
    <regex>
.
.
```

Hier wird jeder LogEintrag zur Verarbeitung herangezogen außer er enthält die Zeichenkette DEBUG

RegEx

Wird eine Map aufgrund Ihres Identifiers ausgewählt, so sind die Attribute-Elemente innerhalb dieses XML Elements dafür zuständig, den Logeintrag in einzelne Teile zu zerlegen und den Feldern eines LogAppEvents zuzuordnen. Dies geschieht je nach gewähltem Modus anders und wird im Abschnitt zu den jeweiligen Modi detaillierter erklärt. Der Aufbau eines Attributelements wird im Anschluss an die Erklärung zu Staticinfo erläutert.

Beispiel:

```
<regex>
    <attribute save="true" name="evt_msg_short">(.*)</attribute>
```

Staticinfo

Staticinfo ist wie auch schon Regex eine Sammlung von Attributelementen. Der Unterschied besteht darin, dass die Felder hierbei nicht mit dynamischen Inhalten aufgrund von Regex befüllt werden, sondern einen statischen Wert enthalten.

Beispiel:

```
</regex>
<staticinfo>
  <attribute save="true" name="log_type">Linux Authentication</attribute>
<staticinfo>
.
.
```

Jedes Event welches aufgrund dieser Parsemap entsteht erhält nun als log_type den Wert “Linux Authentication”

Attribute

Dieses Element ist dafür zuständig, Inhalte in ein Feld des zu erzeugenden LogAppEvents zu speichern.

Im Falle einer Platzierung im Regex Element geschieht dies mit Regex, welche Werte wie genau aus der Log Zeile geparsed werden, hängt hierbei vom Modus ab und ist bei der Beschreibung der verschiedenen Modi nachzulesen.

Sollte das AttributElement im staticinfo Element platziert sein so wird ein statischer Wert verwendet.

Grundsätzlich ist ein Attribut wie folgt aufgebaut. Auf Unterschiede und Spezial Attribute wird bei den jeweiligen Modi eingegangen.

```
<attribute save="true" name="evt_event_id" >log_id=([0-9]+)</attribute>
```

Als Wert hat das Attribut Element eine Regex oder einen statischen String.

Das Attribut save (mögliche Werte true oder false) legt fest ob der Wert gespeichert werden soll.

Im Attribut name wird festgelegt in welche Datenbankspalte der Wert gespeichert wird.

Folgende normalisierte Datenbankspalten stehen als mögliche Werte von name Attributen zur Verfügung:

Datenbankspalte	Beschreibung
evt_timecreated	Beinhaltet Zeitstempel des Originalevents.
log_device_name	Name des Devices, auf welchem die Lognachricht generiert wurde.
log_reference	Speichern der Quelle, aus welchem die Lognachricht gelesen wurde.
log_type	Speichern des Lognachrichtentyps.
log_subtype	Speichern des Lognachrichtensubtyps.
log_evt_writer	Speichern der Information, wer die Lognachricht geschrieben hat. z.B. Provider ,Prozess, Service oder Honeypot-Dienst.
evt_source_ip	Speichern der Quell IP-Adresse.
evt_source_port	Speichern des Quell Ports.
evt_source_info	Speichern von weiteren Quell Infos.
evt_dest_ip	Speichern der Ziel IP-Adresse.
evt_dest_port	Speichern des Ziel Ports.
evt_dest_info	Speichern von weiteren Ziel Infos.
evt_protocol	Verwendetes Protokoll der Lognachricht.
evt_source_user	Speichern von User aus der Lognachricht.
evt_target_object	Speichern des Objekts das bearbeitet, geändert wird.
evt_target_action	Speichern der Aktion die ausgeführt wurde wie z.B. löschen, ändern, hinzufügen, …
evt_msg_short	Speichern der geparsten Lognachricht (aktuell Message-Name).
evt_msg_full	Speichern der geparsten Lognachrichten Details.
evt_msg_raw	Beinhaltet das gesamte Original Event. Wird von LogApp automatisch gespeichert.
evt_priority	Speichern von Priorität, Severity, Level oder ähnlichen Parametern.
evt_event_id	Speichern der Event ID des originalen Events.
evt_keywords	Speichern von zusätzlichen Schlüsselwörtern.

Tabelle 33: Normalisierte Datenbankspalten

Achtung: Wird eine nicht existente Datenbankspalte angegeben, werden die Werte nicht in die Datenbank geschrieben.

Sollte sich in den oben festgehaltenen Spalten keine passende finden, so gibt es die Möglichkeit generische Spalten zu verwenden. Diese sind evt_detail1-evt_detail30.

Um diesen generischen Spalten Namen (Diese können frei gewählt werden) zu geben, ist ein Label notwendig. Labels lassen sich im Menü „Log Quellen“ -> „Labels“ erstellen und verwalten.

Die Zuweisung eines Labels zu einem Event geschieht in der Parsemap mit dem Tag `<labelmapid>ID</labelmapid>`, wobei ID hier für die ID des Labels steht.

Datenbankspalte	Typ	Beschreibung
evt_detail1 – evt_detail20	varchar(255)	Speichern eines weiteren Text Parameters, der nicht in den normalisierten Datenbankspalten definiert ist.
evt_detail21 – evt_detail30	bigint(20)	Speichern eines weiteren Zahlen Parameters, der nicht in den normalisierten Datenbankspalten definiert ist.

Tabelle 34: Datenbankspalten evt_detail1-30

Mithilfe der Attribute anonymize und anonymizeraw ist es Ihnen möglich werte entweder in den einzelnen Feldern (anonymize) oder in der Raw Message zu anonymisieren (anonymizeraw). Hierzu werden Regex gruppe verwendet. Der Wert dieser Attribute entspricht den Gruppennummern der Regex, welche zu anonymisieren ist. Es können auch Listen von Gruppen, getrennt durch Beistrich angegeben werden.

Beispiel:

Logzeile:

```
2014-10-02 11:04:10 Administrator admin login failed from ssh(192.168.50.13) because of invalid password
```

Attribute

```
<attribute save="true" name="evt_msg_short" anonymize="1,2"
anonymizeraw="1">Administrator ([a-zA-Z]*).*beause of(.*)</attribute>
```

Ergebnis:

Datenbankspalte	Inhalt
evt_msg_short	`Administrator *** login failed from ssh(192.168.50.13) because of ***`
evt_msg_raw	`Administrator *** login failed from ssh(192.168.50.13) because of invalid password`

Labelmapid

Wie bei den Attributen bereits erwähnt lassen sich mithilfe von Labels die Spalten evt_detail1-30 benennen.

Hierfür ist lediglich ein XML Element mit dem Wert der ID des zu verwendenden Labels notwendig.

Seperator

Dieses Element ist nur für die Verwendung des CSV Parsingmodus von Nöten. Als Wert wird der Delemiter angegeben, welcher zu Abgrenzung der CSV Spalten herangezogen wird.

Modus zum Parsen von Logfiles:

Webserver Format style

Bei unstrukturierten Logzeilen muss in der Konfigurationsgruppe der Modus WebServer Format style gewählt werden. Folgende beispielhafte Logzeilen lassen sich mit WebServer Format style auswerten:

```
May  3 11:52:45 barracuda barracuda/box_Auth_access:  Info barracuda msyslog:
sshd[21838]: Accepted keyboard-interactive/pam for root from 192.168.80.63 port
9080 ssh2
Feb 13 13:54:24 192.168.0.253 mgr:  SME SSH from 192.168.50.16 - MANAGER Mode
```

In diesem Modus wird die Logzeile von vorne nach hinten geparsed, die Reihenfolge der Attribute in der Parsemap muss daher der Reihenfolge in der Logzeile entsprechen. Die Summe der regulären Ausdrücke in der Parsemap muss den gesamten Logzeileninhalt abdecken. Sollte ein Teil der Logmessage nicht verwendet werden, so ist ein Attribut mit dem Namen trash und einer beliebigen Nummer zu verwenden (Beispiel: <attribute save="true" name="trash1">RegEx</attribute>), dieses Attribut wird nicht in das Event gespeichert.

Beispiel:

Logzeile:

```
date=2014-10-02      time=11:04:10      devname=FG100D-Office      logid=0100032002
msg="Administrator admin login failed from ssh(192.168.50.13) because of invalid
password"
```

ParseMap:

```
<map>
  <identifier>(type=event subtype=system)</identifier>
  <blacklist> </blacklist>
  <regex>
    <attribute save="true" name="trash1">(date=)</attribute>
    <attribute save="true" name="evt_timecreated">(\d{4}(-
\d{1,2}){2})\stime=(\d{1,2}:\d{1,2}:\d{1,2})</attribute>
    <attribute save="true" name="trash2">(devname=)</attribute>
    <attribute save="true" name="log_device_name">([^\s]*)</attribute>
    <attribute save="true" name="trash3">(logid=)</attribute>
     <attribute save="true" name="log_reference">([0-9]*)</attribute>
    <attribute save="true" name="trash5">(.*msg=)</attribute>
    <attribute save="true" name="evt_msg_short">(.*)</attribute>
  </regex>
  <staticinfo>
  </staticinfo>
</map>
```

Ergebnis

Datenbankspalte	Inhalt
evt_timecreated	2014-10-02 11:04:10 (normalisiert anhand des Zeitformats)
log_device_name	192.168.0.254
log_reference	0100032002
evt_msg_short	“Administrator admin login failed from ssh(192.168.50.13) because of invalid password”

Key/Value

Der Modus Key/value ist ähnlich dem WebserverFormatstyle. Der wesentliche Vorteil dieses Modus liegt darin, dass weder die richtige Reihenfolge noch die Vollständigkeit zutreffen müssen. Auch entfallen die trash Attribute, was zu einfacheren und übersichtlicheren Parsemaps führt. Natürlich müssen auch die Logeinträge in einem passenden Format vorliegen. In der Parsemap definierte und nicht vorhandene Keys oder nicht anwendbare reguläre Ausdrücke werden ignoriert.

Folgende beispielhafte Logzeile lässt sich mit Key/Value auswerten:

```
date=2012-05-24 time=10:38:08 devname=FGT300C-RNW device_id=FG300C3911601357
log_id=0038000007 type=traffic subtype=other pri=warning vd=root
src=172.24.101.149 src_port=137 src_int="Client-1" dst=172.24.101.255 dst_port=137
dst_int="root" SN=20953509 status=deny policyid=0 dst_country="Reserved"
service=Windows RPC/Filecopy proto=17 duration=0 sent=0 rcvd=0
msg="iprope_in_check() check failed, drop
```

Ein Attribut im Key/value Format ist wie folgt definiert. Beispiel:

```
    <attribute save="true" name="evt_msg_short">msg="([^"]*)"</attribute>
```

Hierbei wird für die identifizierung die gesamte Regex herangezogen. Als Value wird die erste Gruppe (Im Beispiel grün) herangezogen und als Wert für die Datebankspalte verwendet.

Beispiel:

Logzeile:

```
date=2014-10-02      time=11:04:10      devname=FG100D-Office      logid=0100032002
msg="Administrator admin login failed from ssh(192.168.50.13) because of invalid
password"
```

ParseMap:

```
<map>
  <identifier>(type=event subtype=system)</identifier>
  <regex>
    <attribute save="true" name="evt_timecreated">date=(\d{4}(-
\d{1,2}){2})\stime=(\d{1,2}:\d{1,2}:\d{1,2})</attribute>
    <attribute save="true" name="log_device_name">devname=([^\s]*)</attribute>
     <attribute save="true" name="log_reference">logid=([0-9]*)</attribute>
    <attribute save="true" name="evt_msg_short">msg=(.*)</attribute>
  </regex>
  <staticinfo></staticinfo>
</map>
```

Ergebnis:

Datenbankspalte	Inhalt
evt_timecreated	2014-10-02 11:04:10 (normalisiert anhand des Zeitformats)
log_device_name	192.168.0.254
log_reference	0100032002
evt_msg_short	“Administrator admin login failed from ssh(192.168.50.13) because of invalid password”

XML

Mithilfe des XML Modus lassen sich XML Strukturen, egal ob sie ein oder mehrzeilig sind verarbeiten. Der in der Parsemap definierte Mehrzeilenmodus wird in diesem Parse Modus ignoriert. Die Struktur muss eine gültige XML-Struktur sein, wie zum Beispiel:

```
<logentry date=”2016-09-20 20:45:12”>
<message>Accepted keyboard-interactive/pam for root from 192.168.80.63 port 9080
ssh2<\message>
<\logentry>
```

Für den XML Modus gelten ein paar besondere Eigenheiten. So wird im Identifier statt einer Logzeile der Name des root Elements für den Logeintrag gesucht. Dadurch muss die Regex diesem angepasst werden.

Für die attribute Elemente im Regex Element gilt auch eine Besonderheit. Hier muss ein Attribut mit dem Namen tag verwendet werden. Dieses gibt den Tag/Attributnamen an welcher für die Verarbeitung herangezogen wird. Dieser Name kann auch hierarchisch definiert sein(„/rootElement/subelement1/Subelement2“ z.B. „logentry/ message“) Format:

<attribute save="true" name="evt_msg_short" tag="message">(.*)</attribute>

Die im Wert des attribute enthaltene RegEx liefert nur Werte innerhalb des XMLElements/Attributes zurück.

Beispiel:

Logzeile:

```
<logentry date=”2016-09-20 20:45:12”> <message>Accepted keyboard-interactive/pam
for root from 192.168.80.63 port 9080 ssh2<\message><\logentry>
```

```
ParseMap:
<map>
  <identifier>logentry</identifier>
  <blacklist>
    <!--<blacklist_identifier></blacklist_identifier>-->
  </blacklist>
  <regex>
    <attribute save="true" name="evt_timecreated" tag="date">.*</attribute>
    <attribute save="true" name="evt_msg_short" tag="message">.*</attribute>
  </regex>
  <staticinfo>
  </staticinfo>
  <labelmapid>11</labelmapid>
</map>
```

Ergebnis:

Datenbankspalte	Inhalt
evt_timecreated	2016-09-20 20:45:12 (normalisiert anhand des Zeitformats)
evt_msg_short	Accepted keyboard-interactive/pam for root from 192.168.80.63 port 9080 ssh2

CSV

Dieser Modus erlaubt es, Dateien im CSV Format einfach zu parsen. Hierbei wird der Logeintrag anhand des in der Parsemap definierten Separators in einzelne Felder geteilt.

Beim Abarbeiten iteriert der Agent nun von oben nach unten durch die Attribute, die Reihenfolge der Attribute bestimmt das Feld welches zur verarbeitung herangezogen wird (1. Attribut parsed 1. Feld im CSV, usw.)

Sollte hierbei ein Feld ausgelassen werden so ist ein Attribut zu definieren, welches das save Attribut auf false gesetzt hat.

Im CSV Modus gibt es die Möglichkeit den Identifier wie gewohnt einzusetzen oder aber eine ganz bestimmte Spalte mit dem Attribut column und dem Wert der Spaltennummer anzugeben.

Beispiel:

Logzeile:

```
2016-09-20 20:45:12; Accepted keyboard-interactive/pam for root from
192.168.80.63; port 9080; ssh2
```

```
Parsemap
<map>
  <identifier column=4>ssh2</identifier>
  <blacklist>
  </blacklist>
  <regex>
    <attribute save="true" name="evt_timecreated">.*</attribute>
    <attribute save="true" name="evt_msg_short">.*</attribute>
    <attribute save="false" name="">.*</attribute>
    <attribute save="true" name="evt_protocol">.*</attribute>
  </regex>
  <staticinfo>
  </staticinfo>
  <labelmapid>11</labelmapid>
  <seperator>;</seperator>
</map>
```

Ergebnis:

Datenbankspalte	Inhalt
evt_timecreated	2016-09-20 20:45:12 (normalisiert anhand des Zeitformats)
evt_msg_short	Accepted keyboard-interactive/pam for root from 192.168.80.63
evt_protocol	Ssh2

Default Parsemap

Die folgende Parsemap zeigt den grundlegenden Aufbau und die verfügbaren Settings.

```
<maps>
    <settings>
        <!-- global settings for all maps -->
        <!-- <discardeventsfornotmatchingmap>no</discardeventsfornotmatchingmap> -->
             <!-- use this setting for collecting events, where the matching parsemaps fails to parse
            the event -->
             <!-- values: no: events are collected, full message will show a warning; count: events
            will not be collected, hourly stats will be sent in an event -->
        <!-- <countnotmatchingidentifiers>yes</countnotmatchingidentifiers> -->
        <!-- use this setting for counting events not matching any identifier -->
             <!-- for collecting events not matching any identifier use and wildcard (.*) identifier
            map the very end of the maps -->
        <!-- <countdiscardedeventsblacklist>yes</countdiscardedeventsblacklist> -->
        <!-- use this setting for counting events discarded because of blacklist terms -->
        <!-- for temporary collecting events with blacklist terms disable blacklist terms -->
    </settings>
    <map>
        <!-- name: Generic LinuxLogFile -->
        <!-- path: /var/log/log -->
        <!-- mode: Webserver | Key/Value | CSV | XML -->
        <!-- time format: e.g. dd.MM.yyyy HH:mm:ss -->
        <!-- datetime sample: e.g. 01.02.2013 13:15:00 -->
        <!-- log line sample: e.g. 01.02.2013 13:15:00 this is a log entry. -->
        <settings>
            <!-- <discardeventsfornotmatchingmap>no</discardeventsfornotmatchingmap> -->
                 <!-- use this setting for collecting events, where the matching parsemaps fails to
                parse the event -->
                 <!-- values: no: events are collected, full message will show a warning; count:
                events will not be collected, hourly stats will be sent in an event -->
            <!-- <countnotmatchingidentifiers>yes</countnotmatchingidentifiers> -->
            <!-- use this setting for counting events not matching any identifier -->
                 <!-- for collecting events not matching any identifier use and wildcard (.*)
                identifier map the very end of the maps -->
            <!-- <countdiscardedeventsblacklist>yes</countdiscardedeventsblacklist> -->
            <!-- use this setting for counting events discarded because of blacklist terms -->
            <!-- for temporary collecting events with blacklist terms disable blacklist terms -->
        </settings>
             <!-- define an regex identifier within the line this map should be applied to (Webserver,
            Key/Value, XML) -->
              <identifier>(.*)</identifier>
              <!-- define the column and an regex identifier within the line this map should be
            applied to (CSV) -->
              <!-- <identifier column=5>(asdf|fdsa)</identifier> -->
        <blacklist>
            <!-- Defining blacklisted search terms -->
            <!-- <blacklistidentifier>DEBUG</blacklistidentifier> -->
        </blacklist>
        <regex>
            <!-- Assigning parts of the parsed line to DB attributes (Webserver)-->
            <attribute save="true" name="evt msg short">(.*)</attribute>
            <!-- <attribute save="true" name="evt msg short" anonymize="1,3"
anonymizeraw="1">(\w)\s(\w)\s(\w)\s(.*)</attribute> -->
                     <!-- anonymizes (and replaces it with ***) the first and third RegEx group(word)
in the evt_msg_short field and the first RegEx group(word) in the field evt_msg_raw-->
                     <!-- Assigning parts of the parsed line to DB attributes (Key/Value)-->
              <!-- <attribute save="true" name="evt msg short">msg=(.*)</attribute> -->
                     <!-- Assigning parts of the parsed line to DB attributes (XML)-->
                     <!-- <attribute save="true" name="evt msg short" tag="some XML
                    tag">(.*)</attribute> -->
                     <!-- Assigning parts of the parsed line to DB attributes (CSV)-->
                     <!-- <attribute save="true" name="evt msg short">(.*)</attribute> -->
                     <!-- Skip next element of the parsed line (CSV)-->
                     <!-- <attribute save="false"/> -->
        </regex>
        <staticinfo>
            <!-- Assigning static values to DB attributes -->
            <attribute save="true" name="evt priority">1</attribute>
              <attribute save="true" name="log type">Generic LogFile</attribute>
         </staticinfo>
              <!-- define the seperator for CSV -->
              <!-- <seperator>;</seperator> -->
    </map>
```

```
</maps>
```

Black und Whitelist bei Fileintegritymonitoring

Filter bei Black und Whitelists funktionieren beim Fileintegritymonitoring gleich, nur ist das Ergebnis ein anderes. Bei einem Match bei der Blacklist wird nicht gescanned, bei der Whitelist wird nur gescanned wenn ein Match da ist.

Filter können absolut (C:\Windows\System32) oder relativ zu den in den Pfaden definierten Pfaden angegeben werden. So erzielt schlussendlich ein Filter „System32“, bei einem definierten Pfad von „C:\Windows“ die gleiche Wirkung wie ein Filter „C:\Windows\System32“. Wird ein relativer Filter verwendet, so gilt dieser bei jedem Pfad. Sollten also bei einer ConfigGruppe die Pfade C:\Windows\System32 und C:\Program Files (x86)\ definiert sein, so erzielt ein Filter System32 die gleiche Wirkung wie zwei Filter „C:\Windows\System32“ und „C:\Program Files (x86)\System32“.

Unterschiede zwischen Filter auf Files und Directories

Files

Files können (egal ob absolut oder relativ) mit ganzen Filenamen (authentication.dll bzw C:\Windows\System32\authentication.dll) oder mit einer Wildcard angegeben werden (*.dll bzw. C:\Windows\System32*.dll). Bei einer Wildcard ist es dabei egal ob der ganze Pfad angegeben wird. So kommt es bei einem File „C:\Windows\System32\Auth\authentication.dll“ sowohl bei einem Filter „*.dll“ als auch bei einem Filter „C:\Windows\System32\Auth*.dll“ zu einem Match.

Directories

Im Gegensatz zu den Files gibt es bei Directories keine Wildcard. Der Name des Directories muss (egal ob absolut oder relativ) ganz übergeben werden. Z.b. C:\Windows\System32 oder System32

Beispiele

Pfade	C:\Windows\
Blacklist	System32
Ergebnis	
In diesem Beispiel wird das gesamte „C:\Windows“ Directory gescanned, mit der Ausnahme des Directories „C:\Windows\System32“. Ein File welches den Pfad „C:\Windows\System32.dll“ aufweißt würde jedoch gescanned werden.	

Tabelle 35: Beispiel 1 FIM Black/Whitelist

Pfade	C:\Windows\
Blacklist	C:\Windows\System32
Ergebnis	
Entspricht dem vorangegangenen Beispiel	

Tabelle 36: Beispiel 2 FIM Black/Whitelist

Pfade	C:\Windows\ C:\Temp\
Blacklist	*.dll
Ergebnis	
Die Pfade „C:\Windows\“ und „C:\Temp\“ werden gescanned, jeodch werden alle .dll files ausgenommen.	

Tabelle 37: Beispiel 3 FIM Black/Whitelist

Pfade	C:\Windows\ C:\Temp\
Blacklist	C:\Temp*.dll
Ergebnis	
Die Pfade „C:\Windows\“ und „C:\Temp\“ werden gescanned, jeodch werden alle .dll files im Directorie C:\Temp\ ausgenommen.	

Tabelle 38: Beispiel 4 FIM Black/Whitelist

SNMP Abfragen mittels OID

Die folgende Tabelle zeigt die verfügbaren OIDs, die über SNMP abgefragt werden können. Der nachstehende Befehl zeigt ein Beispiel für die Abfrage in Version 2.

snmpget -v2c -Os -c [community] [IP-LogApp eth0] 1.3.6.1.4.1.2021.11.9.0

Name	OID
Cdavis	1.3.6.1.4.1.2021
laTable	1.3.6.1.4.1.2021.10
laEntry	1.3.6.1.4.1.2021.10.1
laIndex	1.3.6.1.4.1.2021.10.1.1.1
laErrorFlag	1.3.6.1.4.1.2021.10.1.100.1
laErrMessage	1.3.6.1.4.1.2021.10.1.101.1
laNames	1.3.6.1.4.1.2021.10.1.2.1
laLoad	1.3.6.1.4.1.2021.10.1.3.1
laConfig	1.3.6.1.4.1.2021.10.1.4.1
laLoadInt	1.3.6.1.4.1.2021.10.1.5.1
laLoadFloat	1.3.6.1.4.1.2021.10.1.6.1
systemStats	1.3.6.1.4.1.2021.11
ssIndex	1.3.6.1.4.1.2021.11.1.0
ssCpuSystem	1.3.6.1.4.1.2021.11.10.0
ssCpuIdle	1.3.6.1.4.1.2021.11.11.0
ssErrorName	1.3.6.1.4.1.2021.11.2.0
ssSwapIn	1.3.6.1.4.1.2021.11.3.0
ssSwapOut	1.3.6.1.4.1.2021.11.4.0
ssIOSent	1.3.6.1.4.1.2021.11.5.0
ssCpuRawUser	1.3.6.1.4.1.2021.11.50.0
ssCpuRawNice	1.3.6.1.4.1.2021.11.51.0
ssCpuRawSystem	1.3.6.1.4.1.2021.11.52.0
ssCpuRawIdle	1.3.6.1.4.1.2021.11.53.0
ssCpuRawWait	1.3.6.1.4.1.2021.11.54.0
ssCpuRawKernel	1.3.6.1.4.1.2021.11.55.0
ssCpuRawInterrupt	1.3.6.1.4.1.2021.11.56.0
ssIORawSent	1.3.6.1.4.1.2021.11.57.0
ssIORawReceived	1.3.6.1.4.1.2021.11.58.0
ssRawInterrupts	1.3.6.1.4.1.2021.11.59.0
ssIOReceive	1.3.6.1.4.1.2021.11.6.0
ssRawContexts	1.3.6.1.4.1.2021.11.60.0
ssCpuRawSoftIRQ	1.3.6.1.4.1.2021.11.61.0
ssRawSwapIn	1.3.6.1.4.1.2021.11.62.0
ssRawSwapOut	1.3.6.1.4.1.2021.11.63.0
ssCpuRawSteal	1.3.6.1.4.1.2021.11.64.0
ssCpuRawGuest	1.3.6.1.4.1.2021.11.65.0

ssCpuRawGuestNice	1.3.6.1.4.1.2021.11.66.0
ssSysInterrupts	1.3.6.1.4.1.2021.11.7.0
ssSysContext	1.3.6.1.4.1.2021.11.8.0
ssCpuUser	1.3.6.1.4.1.2021.11.9.0
memory	1.3.6.1.4.1.2021.4
memIndex	1.3.6.1.4.1.2021.4.1.0
memAvailRealTXT	1.3.6.1.4.1.2021.4.10.0
memSwapError	1.3.6.1.4.1.2021.4.100.0
memSwapErrorMsg	1.3.6.1.4.1.2021.4.101.0
memTotalFree	1.3.6.1.4.1.2021.4.11.0
memMinimumSwap	1.3.6.1.4.1.2021.4.12.0
memShared	1.3.6.1.4.1.2021.4.13.0
memBuffer	1.3.6.1.4.1.2021.4.14.0
memCached	1.3.6.1.4.1.2021.4.15.0
memErrorName	1.3.6.1.4.1.2021.4.2.0
memTotalSwap	1.3.6.1.4.1.2021.4.3.0
memAvailSwap	1.3.6.1.4.1.2021.4.4.0
memTotalReal	1.3.6.1.4.1.2021.4.5.0
memAvailReal	1.3.6.1.4.1.2021.4.6.0
memTotalSwapTXT	1.3.6.1.4.1.2021.4.7.0
memAvailSwapTXT	1.3.6.1.4.1.2021.4.8.0
memTotalRealTXT	1.3.6.1.4.1.2021.4.9.0
dskTable	1.3.6.1.4.1.2021.9
dskEntry **9.1.*.1 für „/“** **9.1.*.2 für „/var“**	1.3.6.1.4.1.2021.9.1
dskIndex	1.3.6.1.4.1.2021.9.1.1.1
dskIndex	1.3.6.1.4.1.2021.9.1.1.2
dskPath	1.3.6.1.4.1.2021.9.1.2.1
dskPath	1.3.6.1.4.1.2021.9.1.2.2
dskDevice	1.3.6.1.4.1.2021.9.1.3.1
dskDevice	1.3.6.1.4.1.2021.9.1.3.2
dskMinimum	1.3.6.1.4.1.2021.9.1.4.1
dskMinimum	1.3.6.1.4.1.2021.9.1.4.2
dskMinPercent	1.3.6.1.4.1.2021.9.1.5.1
dskMinPercent	1.3.6.1.4.1.2021.9.1.5.2
dskTotal	1.3.6.1.4.1.2021.9.1.6.1
dskTotal	1.3.6.1.4.1.2021.9.1.6.2
dskAvail	1.3.6.1.4.1.2021.9.1.7.1
dskAvail	1.3.6.1.4.1.2021.9.1.7.2
dskUsed	1.3.6.1.4.1.2021.9.1.8.1
dskUsed	1.3.6.1.4.1.2021.9.1.8.2
dskPercent	1.3.6.1.4.1.2021.9.1.9.1
dskPercent	1.3.6.1.4.1.2021.9.1.9.2

dskPercentNode	1.3.6.1.4.1.2021.9.1.10.1
dskPercentNode	1.3.6.1.4.1.2021.9.1.10.2
dskTotalLow	1.3.6.1.4.1.2021.9.1.11.1
dskTotalLow	1.3.6.1.4.1.2021.9.1.11.2
dskTotalHigh	1.3.6.1.4.1.2021.9.1.12.1
dskTotalHigh	1.3.6.1.4.1.2021.9.1.12.2
dskAvailLow	1.3.6.1.4.1.2021.9.1.13.1
dskAvailLow	1.3.6.1.4.1.2021.9.1.13.2
dskAvailHigh	1.3.6.1.4.1.2021.9.1.14.1
dskAvailHigh	1.3.6.1.4.1.2021.9.1.14.2
dskUsedLow	1.3.6.1.4.1.2021.9.1.15.1
dskUsedLow	1.3.6.1.4.1.2021.9.1.15.2
dskUsedHigh	1.3.6.1.4.1.2021.9.1.16.1
dskUsedHigh	1.3.6.1.4.1.2021.9.1.16.2
dskErrorFlag	1.3.6.1.4.1.2021.9.1.100.1
dskErrorFlag	1.3.6.1.4.1.2021.9.1.100.2
dskErrorMsg	1.3.6.1.4.1.2021.9.1.101.1
dskErrorMsg	1.3.6.1.4.1.2021.9.1.101.2
LogApp Mibs	1.3.6.1.4.1.8072.1.3.2.4.1.2.2
System - Human readable	1.3.6.1.4.1.8072.1.3.2.4.1.2.2.65.65
CPU usage	1.3.6.1.4.1.8072.1.3.2.4.1.2.2.65.65.1
Memory Usage	1.3.6.1.4.1.8072.1.3.2.4.1.2.2.65.65.2
HDD System total	1.3.6.1.4.1.8072.1.3.2.4.1.2.2.65.65.3
HDD System used	1.3.6.1.4.1.8072.1.3.2.4.1.2.2.65.65.4
HDD System used (%)	1.3.6.1.4.1.8072.1.3.2.4.1.2.2.65.65.5
HDD System free	1.3.6.1.4.1.8072.1.3.2.4.1.2.2.65.65.6
HDD DB total	1.3.6.1.4.1.8072.1.3.2.4.1.2.2.65.65.7
HDD DB used	1.3.6.1.4.1.8072.1.3.2.4.1.2.2.65.65.8
HDD DB used (%)	1.3.6.1.4.1.8072.1.3.2.4.1.2.2.65.65.9
HDD DB free	1.3.6.1.4.1.8072.1.3.2.4.1.2.2.65.65.10
DB Data used	1.3.6.1.4.1.8072.1.3.2.4.1.2.2.65.65.11
DB Data used (%)	1.3.6.1.4.1.8072.1.3.2.4.1.2.2.65.65.12
DB File used	1.3.6.1.4.1.8072.1.3.2.4.1.2.2.65.65.13
DB File used (%)	1.3.6.1.4.1.8072.1.3.2.4.1.2.2.65.65.14
Additional Files used	1.3.6.1.4.1.8072.1.3.2.4.1.2.2.65.65.15
Additional Files used (%)	1.3.6.1.4.1.8072.1.3.2.4.1.2.2.65.65.16
System - Numbers only	1.3.6.1.4.1.8072.2.255.2.1.2.2.65.66
CPU usage	1.3.6.1.4.1.8072.2.255.2.1.2.2.65.66.1
Memory Usage	1.3.6.1.4.1.8072.2.255.2.1.2.2.65.66.2
HDD System total (KB)	1.3.6.1.4.1.8072.2.255.2.1.2.2.65.66.3
HDD System used (KB)	1.3.6.1.4.1.8072.2.255.2.1.2.2.65.66.4
HDD System used (%)	1.3.6.1.4.1.8072.2.255.2.1.2.2.65.66.5
HDD System free (KB)	1.3.6.1.4.1.8072.2.255.2.1.2.2.65.66.6
HDD DB total (KB)	1.3.6.1.4.1.8072.2.255.2.1.2.2.65.66.7
HDD DB used (KB)	1.3.6.1.4.1.8072.2.255.2.1.2.2.65.66.8
HDD DB used (%)	1.3.6.1.4.1.8072.2.255.2.1.2.2.65.66.9
HDD DB free (KB)	1.3.6.1.4.1.8072.2.255.2.1.2.2.65.66.10
DB Data used (KB)	1.3.6.1.4.1.8072.2.255.2.1.2.2.65.66.11
DB Data used (%)	1.3.6.1.4.1.8072.2.255.2.1.2.2.65.66.12
DB File used (KB)	1.3.6.1.4.1.8072.2.255.2.1.2.2.65.66.13

DB File used (%)	1.3.6.1.4.1.8072.2.255.2.1.2.2.65.66.14
Additional Files used (KB)	1.3.6.1.4.1.8072.2.255.2.1.2.2.65.66.15
Additional Files used (%)	1.3.6.1.4.1.8072.2.255.2.1.2.2.65.66.16
LogApp Service - Human readable	1.3.6.1.4.1.8072.1.3.2.4.1.2.2.66.65.
GUI	1.3.6.1.4.1.8072.1.3.2.4.1.2.2.66.65.1
DB	1.3.6.1.4.1.8072.1.3.2.4.1.2.2.66.65.2
Indexer	1.3.6.1.4.1.8072.1.3.2.4.1.2.2.66.65.3
Sshd	1.3.6.1.4.1.8072.1.3.2.4.1.2.2.66.65.4
Receiver	1.3.6.1.4.1.8072.1.3.2.4.1.2.2.66.65.5
FileIntegrity	1.3.6.1.4.1.8072.1.3.2.4.1.2.2.66.65.6
Heartbeat	1.3.6.1.4.1.8072.1.3.2.4.1.2.2.66.65.7
AlertParser	1.3.6.1.4.1.8072.1.3.2.4.1.2.2.66.65.8
ReportingEngine	1.3.6.1.4.1.8072.1.3.2.4.1.2.2.66.65.9
LocalNetworkProxy	1.3.6.1.4.1.8072.1.3.2.4.1.2.2.66.65.10
EventForwarder	1.3.6.1.4.1.8072.1.3.2.4.1.2.2.66.65.11
LogApp Service - Numbers only (0: running; 1: stopped)	1.3.6.1.4.1.8072.2.255.2.1.2.2.66.66.
GUI	1.3.6.1.4.1.8072.2.255.2.1.2.2.66.66.1
DB	1.3.6.1.4.1.8072.2.255.2.1.2.2.66.66.2
Indexer	1.3.6.1.4.1.8072.2.255.2.1.2.2.66.66.3
Sshd	1.3.6.1.4.1.8072.2.255.2.1.2.2.66.66.4
Receiver	1.3.6.1.4.1.8072.2.255.2.1.2.2.66.66.5
FileIntegrity	1.3.6.1.4.1.8072.2.255.2.1.2.2.66.66.6
Heartbeat	1.3.6.1.4.1.8072.2.255.2.1.2.2.66.66.7
AlertParser	1.3.6.1.4.1.8072.2.255.2.1.2.2.66.66.8
ReportingEngine	1.3.6.1.4.1.8072.2.255.2.1.2.2.66.66.9
LocalNetworkProxy	1.3.6.1.4.1.8072.2.255.2.1.2.2.66.66.10
EventForwarder	1.3.6.1.4.1.8072.2.255.2.1.2.2.66.66.11
Indexer stats - Human readable	1.3.6.1.4.1.8072.1.3.2.4.1.2.2.67.65.
Indexer status	1.3.6.1.4.1.8072.1.3.2.4.1.2.2.67.65.1
Health status	1.3.6.1.4.1.8072.1.3.2.4.1.2.2.67.65.2
Indexer size	1.3.6.1.4.1.8072.1.3.2.4.1.2.2.67.65.3
Indexer stats - Numbers only	1.3.6.1.4.1.8072.2.255.2.1.2.2.67.66.
Indexer status (0: running; 1: stopped)	1.3.6.1.4.1.8072.2.255.2.1.2.2.67.66.1
Health status (0: OK, 1: Warning, 2: Error)	1.3.6.1.4.1.8072.2.255.2.1.2.2.67.66.2
Indexer size (KB)	1.3.6.1.4.1.8072.2.255.2.1.2.2.67.66.3
Client stats - Human readbale	1.3.6.1.4.1.8072.2.255.1.2.68.[64+ClientID].65
Total Events for this Client	1.3.6.1.4.1.8072.2.255.1.2.68.[64+ClientID].65.1
Agents offline	1.3.6.1.4.1.8072.2.255.1.2.68.[64+ClientID].65.2
Events last Longterm-Archive	1.3.6.1.4.1.8072.2.255.1.2.68.[64+ClientID].65.3
Duration last Longterm-Archive (sec)	1.3.6.1.4.1.8072.2.255.1.2.68.[64+ClientID].65.4
Agentlist	1.3.6.1.4.1.8072.2.255.1.2.68.[64+ClientID].65.5
Agentnumber	1.3.6.1.4.1.8072.2.255.1.2.68.[64+ClientID].65.5.[Agent#]
Name	1.3.6.1.4.1.8072.2.255.1.2.68.[64+ClientID].65.5.[Agent#].1
IP-Address	1.3.6.1.4.1.8072.2.255.1.2.68.[64+ClientID].65.5.[Agent#].2
Version	1.3.6.1.4.1.8072.2.255.1.2.68.[64+ClientID].65.5.[Agent#].3
Status	1.3.6.1.4.1.8072.2.255.1.2.68.[64+ClientID].65.5.[Agent#].4
Config Groups (heading) /	1.3.6.1.4.1.8072.2.255.1.2.68.[64+ClientID].65.5.[Agent#].5

Proxy ID	
Config Groupy ID	1.3.6.1.4.1.8072.2.255.1.2.68.[64+ClientID].65.5.[Agent#].5.x
Device Class ID	1.3.6.1.4.1.8072.2.255.1.2.68.[64+ClientID].65.5.[Agent#].6
Last Event per Config Group (heading)	1.3.6.1.4.1.8072.2.255.1.2.68.[64+ClientID].65.5.[Agent#].7
Config Groupy ID	1.3.6.1.4.1.8072.2.255.1.2.68.[64+ClientID].65.5.[Agent#].7.x
Seconds since last Event	1.3.6.1.4.1.8072.2.255.1.2.68.[64+ClientID].65.5.[Agent#].7.x.1
Events in the last minute (heading)	1.3.6.1.4.1.8072.2.255.1.2.68.[64+ClientID].65.5.[Agent#].8
Config Groupy ID	1.3.6.1.4.1.8072.2.255.1.2.68.[64+ClientID].65.5.[Agent#].8.x
Number of Events in the last minute	1.3.6.1.4.1.8072.2.255.1.2.68.[64+ClientID].65.5.[Agent#].8.x.1
Events in the last hour (heading)	1.3.6.1.4.1.8072.2.255.1.2.68.[64+ClientID].65.5.[Agent#].9
Config Groupy ID	1.3.6.1.4.1.8072.2.255.1.2.68.[64+ClientID].65.5.[Agent#].9.x
Number of Events in the last hour	1.3.6.1.4.1.8072.2.255.1.2.68.[64+ClientID].65.5.[Agent#].9.x.1
Events in the last day (heading)	1.3.6.1.4.1.8072.2.255.1.2.68.[64+ClientID].65.5.[Agent#].10
Config Groupy ID	1.3.6.1.4.1.8072.2.255.1.2.68.[64+ClientID].65.5.[Agent#].10.x
Number of Events in the last day	1.3.6.1.4.1.8072.2.255.1.2.68.[64+ClientID].65.5.[Agent#].10.x.1
Seconds since last Heartbeat	1.3.6.1.4.1.8072.2.255.1.2.68.[64+ClientID].65.5.[Agent#].11
Client stats - Numbers only	
Total Events for this Client	1.3.6.1.4.1.8072.2.255.2.1.2.2.68.[64+ClientID].65.1
Agents offline	1.3.6.1.4.1.8072.2.255.2.1.2.2.68.[64+ClientID].65.2
Events last Longterm-Archive	1.3.6.1.4.1.8072.2.255.2.1.2.2.68.[64+ClientID].65.3
Duration last Longterm-Archive (sec)	1.3.6.1.4.1.8072.2.255.2.1.2.2.68.[64+ClientID].65.4
Number of Agents	1.3.6.1.4.1.8072.2.255.2.1.2.2.68.[64+ClientID].65.5
Agentnumber	1.3.6.1.4.1.8072.2.255.2.1.2.2.68.[64+ClientID].65.5.[Agent#]
Agent ID	1.3.6.1.4.1.8072.2.255.2.1.2.2.68.[64+ClientID].65.5.[Agent#].1
IP-Address	1.3.6.1.4.1.8072.2.255.2.1.2.2.68.[64+ClientID].65.5.[Agent#].2
Version	1.3.6.1.4.1.8072.2.255.2.1.2.2.68.[64+ClientID].65.5.[Agent#].3
Status (1: Heartbeat-only, 2: Forwarding)	1.3.6.1.4.1.8072.2.255.2.1.2.2.68.[64+ClientID].65.5.[Agent#].4
Number of Config Groups / Proxy ID	1.3.6.1.4.1.8072.2.255.2.1.2.2.68.[64+ClientID].65.5.[Agent#].5
Config Groupy ID	1.3.6.1.4.1.8072.2.255.2.1.2.2.68.[64+ClientID].65.5.[Agent#].5.x
Device Class ID	1.3.6.1.4.1.8072.2.255.2.1.2.2.68.[64+ClientID].65.5.[Agent#].6
Last Event per Config Group (placeholder=0)	1.3.6.1.4.1.8072.2.255.2.1.2.2.68.[64+ClientID].65.5.[Agent#].7
Config Groupy ID	1.3.6.1.4.1.8072.2.255.2.1.2.2.68. [64+ClientID].65.5.[Agent#].7.x
Seconds since last Event	1.3.6.1.4.1.8072.2.255.2.1.2.2.68. [64+ClientID].65.5.[Agent#].7.x.1
Events in the last minute (placeholder=1)	1.3.6.1.4.1.8072.2.255.2.1.2.2.68.[64+ClientID].65.5.[Agent#].8

Config Groupy ID	1.3.6.1.4.1.8072.2.255.2.1.2.2.68. [64+ClientID].65.5.[Agent#].8.x
Number of Events in the last minute	1.3.6.1.4.1.8072.2.255.2.1.2.2.68. [64+ClientID].65.5.[Agent#].8.x.1
Events in the last hour (placeholder=60)	1.3.6.1.4.1.8072.2.255.2.1.2.2.68.[64+ClientID].65.5.[Agent#].9
Config Groupy ID	1.3.6.1.4.1.8072.2.255.2.1.2.2.68. [64+ClientID].65.5.[Agent#].9.x
Number of Events in the last hour	1.3.6.1.4.1.8072.2.255.2.1.2.2.68. [64+ClientID].65.5.[Agent#].9.x.1
Events in the last day (placeholder=1440)	1.3.6.1.4.1.8072.2.255.2.1.2.2.68.[64+ClientID].65.5.[Agent#].10
Config Groupy ID	1.3.6.1.4.1.8072.2.255.2.1.2.2.68. [64+ClientID].65.5.[Agent#].10.x
Number of Events in the last day	1.3.6.1.4.1.8072.2.255.2.1.2.2.68. [64+ClientID].65.5.[Agent#].10.x.1
Seconds since last heartbeat	1.3.6.1.4.1.8072.2.255.2.1.2.2.68.[64+ClientID].65.5.[Agent#].11

Tabelle 39:SNMP Abfragen mittels OIDs

Vergrößerung der virtuellen Festplatte

Werden die aktuellen HDD-Kapazitäten zu gering, besteht die Möglichkeit dieser zu erweitern. Dies kann mit Hilfe der CLI (siehe Abschnitt 5.7) durchgeführt werden. Mit Hilfe des CLI-Kommandos „fdisk –l“ können alle aktuellen Partitionen dargestellt werden.

```
LogApp # fdisk -l
Disk /dev/mapper/vg_db-var doesn't contain a valid partition table

Disk /dev/sda: 42.9 GB, 42949672960 bytes
255 heads, 63 sectors/track, 5221 cylinders, total 83886080 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x00046a55

   Device Boot      Start         End      Blocks   Id  System
/dev/sda1   *        2048     6287359     3142656   82  Linux swap / Solaris
/dev/sda2         6289406    83884031    38797313    5  Extended
/dev/sda5         6289408    30701567    12206080   83  Linux
/dev/sda6        30703616    83884031    26590208   8e  Linux LVM

Disk /dev/mapper/vg_db-var: 27.2 GB, 27225227264 bytes
255 heads, 63 sectors/track, 3309 cylinders, total 53174272 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x00000000
```

Abbildung 128: Auflistung aller Partitionen

Achtung:

- IQSol empfiehlt ein Backup der virtuellen Maschine bevor die Größe der virtuellen Festplatte verändert wird!
- Es wird darauf hingewiesen, dass bei falscher Handhabung dies zum Datenverlust führen kann.
- Um die Vergrößerung der virtuellen Festplatte durchführen zu können, muss die erst Installation der LogApp mit einer HDD Größe von mindestens 40GB durchgeführt worden sein.
- Sollte die Disk bereits zwei Mal erweitert worden sein, so muss eine zweite Festplatte hinzugefügt werden. An der im Folgenden beschriebenen Vorgehensweise ändert dies nur die Bezeichnung des Drives (sdb statt sda)

Im ersten Schritt wird die Größe der virtuellen Festplatte erhöht. Dies kann zum Beispiel bei ESXI-Umgebungen, wie in der nachstehenden Abbildung dargestellt, durchgeführt werden. Die VM muss dazu gestoppt werden.

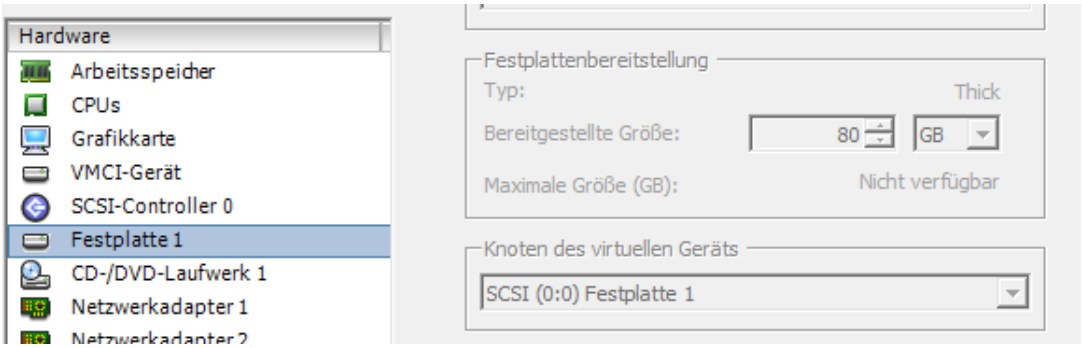

Abbildung 129: Größe der virtuellen Festplatte anpassen

Nach der Anpassung der Größe in den VM-Settings kann die LogApp wieder gestartet werden und mit den nachfolgenden Befehlen die Vergrößerung der virtuellen Festplatte durchgeführt werden.

In der CLI kann mit dem Kommando „cfdisk /dev/sda“ der freie Speicherplatz angezeigt werden.

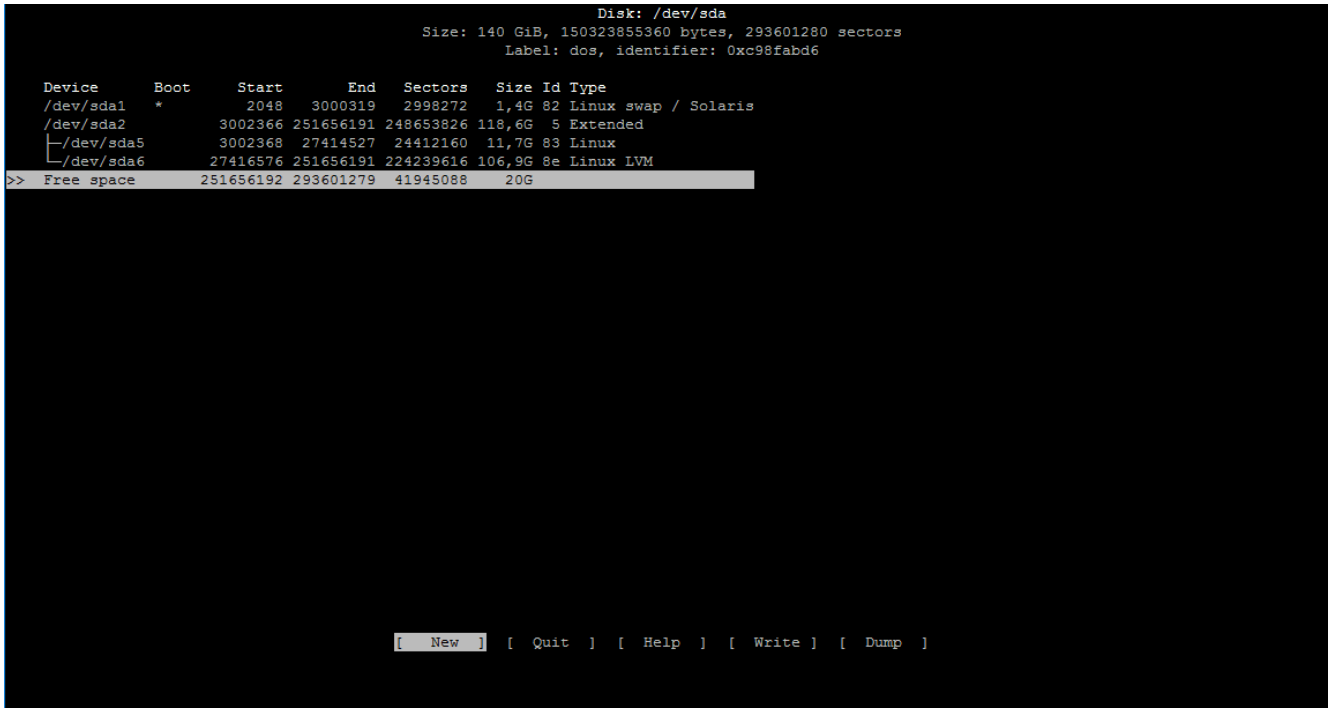

Abbildung 130: Selektieren des freien HDD-Speichers

Den freien Speicher unter Device (Free Space) selektieren und „New“ bestätigen (Enter-Taste).

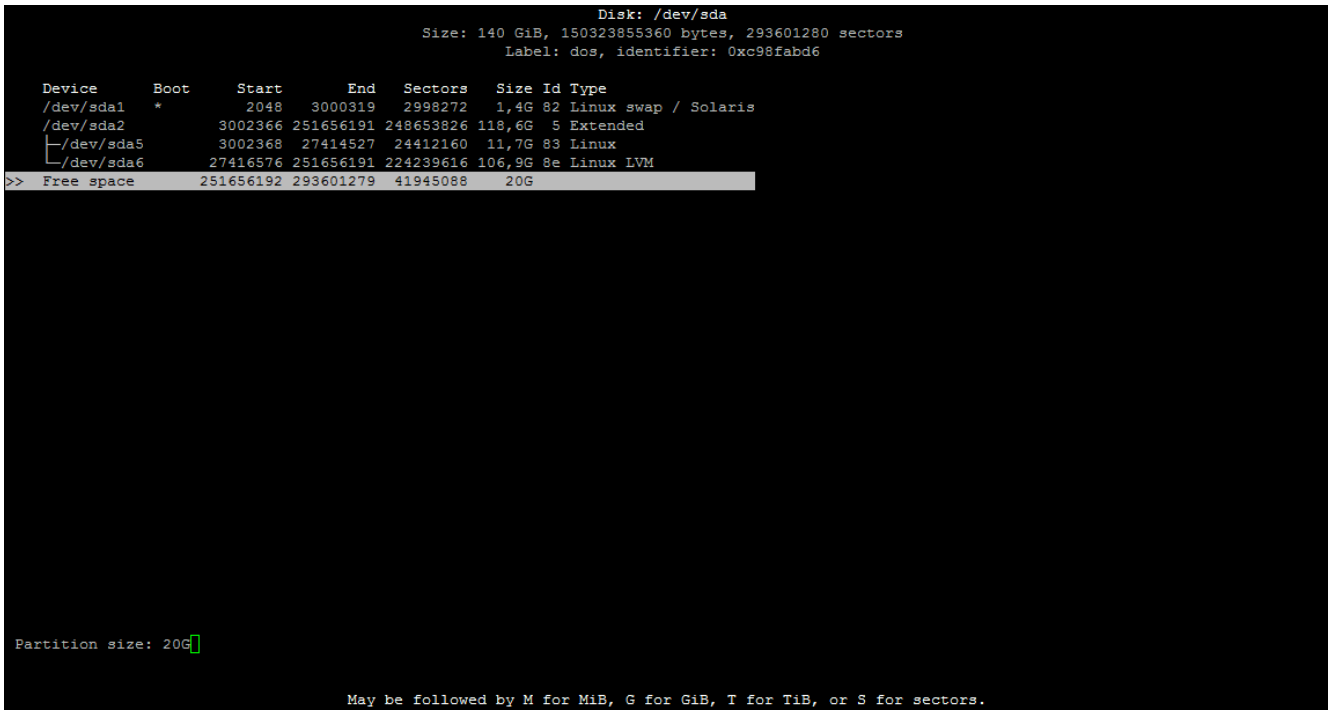

Abbildung 131: Auswahl der Größe

Anschließend wird die Größe ausgewählt und ebenfalls bestätigt.

Anschließend muss im unteren Bereich der Typ festgelgt werden, hier ist Linux LVM zu wählen.

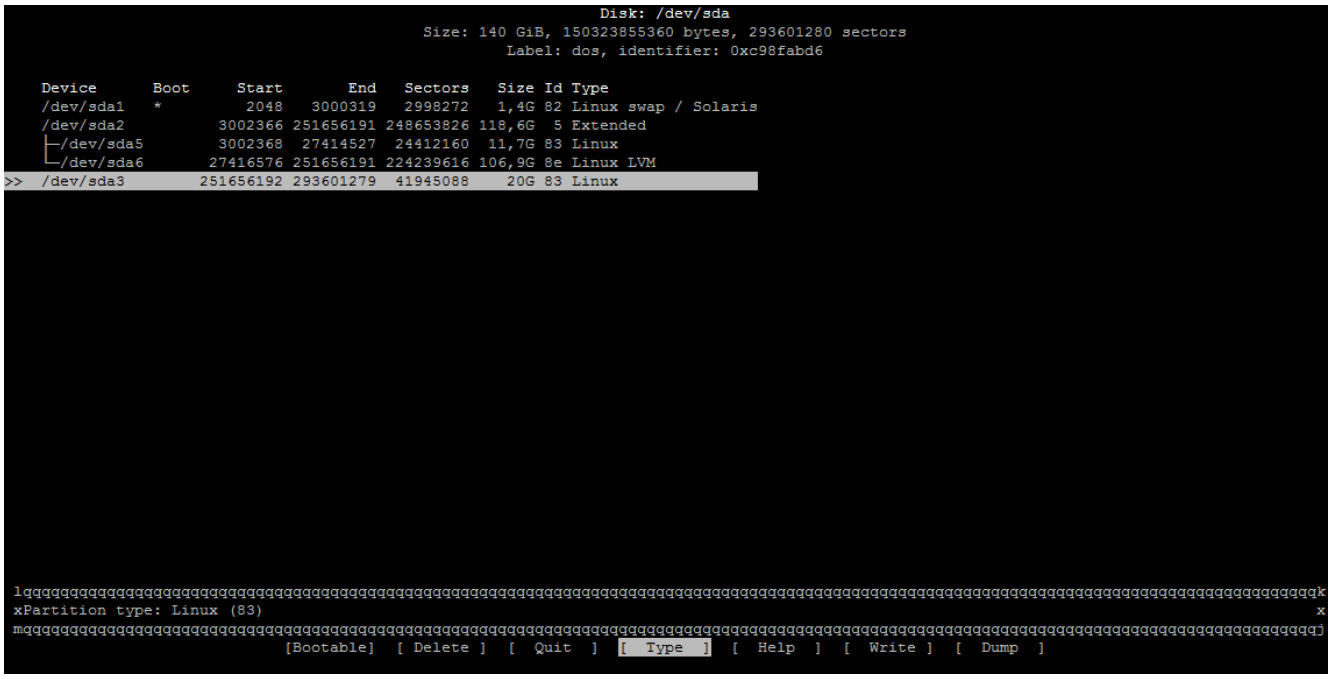

Abbildung 132: Auswahl des Partitionstypen

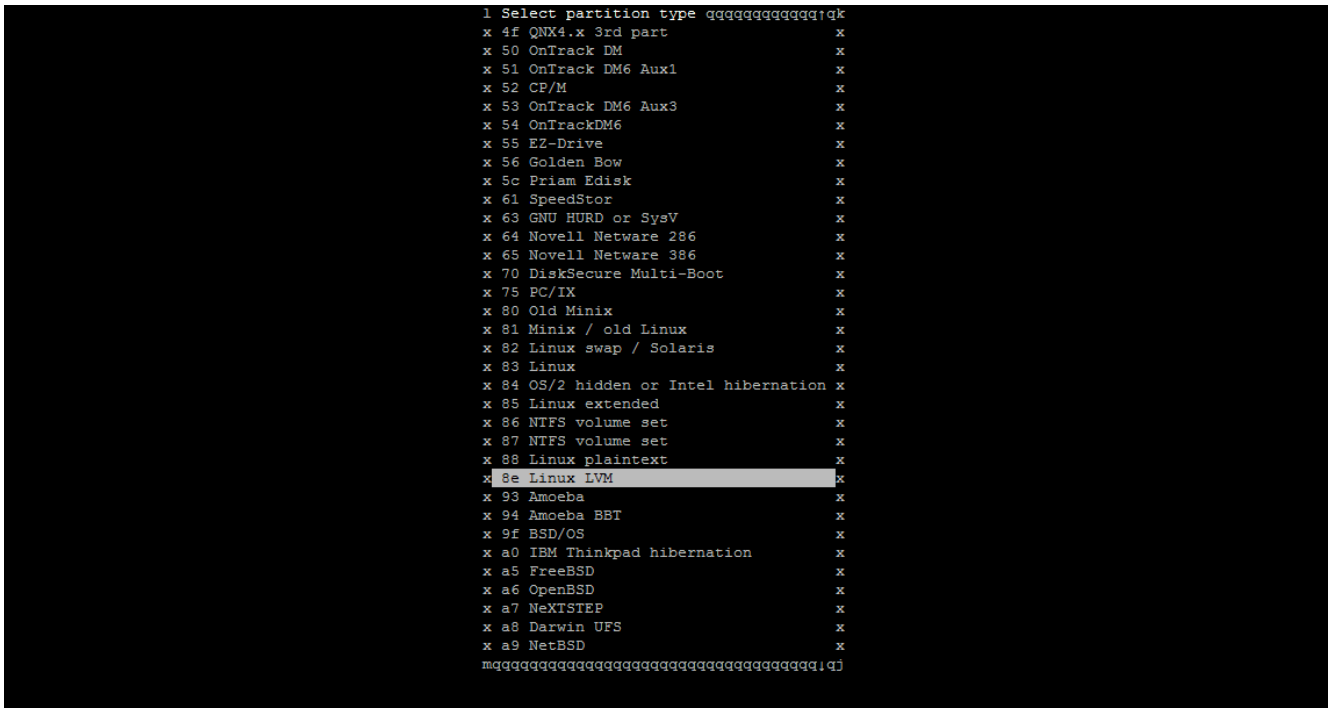

Abbildung 133: Auswahl des Partitionstypen 2

Zuletzt muss die Änderung an der Partitionstabelle mit Write (unterer Bereich) und einer anschießenden Bestätigung gespeichert werden. Mit Quit steigen sie aus dem Programm aus.

Hinweis: Hier können auch Partitionen gelöscht werden, dies führt zu Datenverlust.

Um die neue Partitionstabelle zu laden und die neue Partition zu verwenden, starten sie die LogApp neu.

Nachdem die LogApp neu gestartet ist, kann mit „fdisk –l“ wiederum die neu angelegte Partition aufgelistet werden.

Um diese Partition nun dem LVM zuzuordnen muss als erstes ein physikalisches Volumen angelegt werden.

```
pvcreate /dev/sda[Nummer der neu angelegten Partition]
```

```
LogApp # pvcreate /dev/sda7
  Physical volume "/dev/sda7" successfully created
```

Abbildung 134: Erstellung des physikalisches Volumes

Als nächstes muss die Volume Group vg_db um das physikalische Volume erweitert werden.

```
vgextend vg_db /dev/sda[Nummer der neu angelegten Partition]
```

```
LogApp # vgextend vg_db /dev/sda7
  Volume group "vg_db" successfully extended
```

Abbildung 135: Hinzufügen zur Volume Group

Anschließend muss noch das Logical Volume erweitert werden.

```
lvextend -L+[Anzahl der zu erweiternden GB]G /dev/mapper/vg_db-var
```

```
LogApp # lvextend -L+3G /dev/mapper/vg_db-var
  Extending logical volume var to 28,36 GiB
  Logical volume var successfully resized
```

Abbildung 136: Logisches Volume erweitern

Abschließend muss dem Dateisystem noch mitgeteilt werden, dass es sich anpassen soll. Dies wird mit folgendem Befehl getan.

```
resize2fs /dev/mapper/vg_db-var
```

```
LogApp # resize2fs /dev/mapper/vg_db-var
resize2fs 1.42.9 (4-Feb-2014)
Das Dateisystem auf /dev/mapper/vg_db-var ist auf /var eingehängt; Online-Grössenveränderung nötig
old_desc_blocks = 2, new_desc_blocks = 2
Das Dateisystem auf /dev/mapper/vg_db-var ist nun 7433216 Blöcke groß.
```

Abbildung 137: Dateisystem erweitern

Konfigurieren von Syslog für Linux Agents ohne root-Rechte

Falls ein Linux Agent mit anderen Benutzern als root gestartet wird, kann dieser Agent auf Ports unter 1024 nicht zugreifen, um Syslog-Nachrichten zu empfangen. Folgende Möglichkeiten stehen zur Verfügung, um in solchen Fällen Ports unter 1024 nutzen zu können.

1) Umleitung des Ports

Den Syslog-Port des SensorAgent auf 10514 konfigurieren.

Folgende Befehle ausführen:

```
sudo iptables -t nat -A PREROUTING -p UDP -m udp --dport 514 -j REDIRECT --to-
ports 10514
sudo iptables-save > /etc/iptables.rules
```

1.1) UBUNTU

Die Datei "/etc/network/if-pre-up.d/iptables" mit dem nachfolgenden Inhalt erstellen:

```
#!/bin/sh
iptables-restore < /etc/iptables.rules
exit 0
```

Die Datei "/etc/network/if-post-down.d/iptables" mit dem nachfolgenden Inhalt erstellen:

```
#!/bin/sh
iptables-save > /etc/iptables.rules
exit 0
```

Folgende Befehle ausführen:

```
sudo chmod +x /etc/network/if-post-down.d/iptables
sudo chmod +x /etc/network/if-pre-up.d/iptables
```

1.2) CENTOS

Die Datei "/etc/sysconfig/network-scripts/ifup-post" mit folgenden Befehl ergänzen:

```
iptables-restore < /etc/iptables.rules
```

Die Datei "/etc/sysconfig/network-scripts/ifdown-post" mit folgenden Befehl ergänzen:

```
iptables-save > /etc/iptables.rules
```

2) Weiterleitung über RSYSLOG

Den Syslog-Port des SensorAgent auf 10514 konfigurieren.

In der Datei "/etc/rsyslog.conf" auf folgende Zeilen prüfen:

```
# provides UDP syslog reception
$ModLoad imudp
$UDPServerRun 514
```

In der Datei "/etc/rsyslog.d/50-default.conf" folgende Zeile ergänzen

(IP-Adresse entsprechend dem Empfänger anpassen):

```
*.*             @192.168.80.212:10514
```

Folgenden Befehl ausführen:

```
service rsyslog restart
```

Einrichten von SELinux

Security Ehanced Linux ist eine Erweiterung des Kernels, die anhand von Regeln festlegt, dass gewisse Prozesse nur auf gewisse Regeln zugreifen könne.

Ein LinuxAgent kann in einer von solchen Regeln definierten Confined Damoin betrieben werden.

Für den Betrieb von SELinux sind folgende Pakete nötig:

- yum install policycoreutils-python-utils
- yum install setroubleshoot-server
- yum install policycoreutils

Ist der LogAgent installiert, so kann mit folgendem Befehl kontrolliert werden, ob dieser in der unconfined Domain läuft:

```
ps -efZ | grep Agent

unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 root 443922 1 0 Feb23 ?
00:01:48 /opt/logagent/ManagementAgent
```

Als erstes sind folgende Befehl auszuführen:

sepolicy generate --init /opt/logagent/ManagementAgent

restorecon -v /opt/logagent/ManagementAgent /usr/lib/systemd/system

Diese Befehle legen ein File an (ManagementAgent.te), welches die Regeln enthält.

Mit „./ManagementAgent.sh“ wird anschließend die Policy erstellt.

Wird anschließend der Agent neu gestartet, so kann mit dem oben erwähnten ps Befehl kontorlliert werden, ob der Agent nun in einer confined Domain läuft.

Troubleshooting:

Sollte es bei der Erstellung von Regeln Schwierigkeiten geben, so können folgende Befehle nützlich sein:

- **ausearch -m AVC -ts recent**: Gibt Alerts aus, weche anzeigen, dass sein Prozess versucht hat gegen die difinierten Regeln zu verstoßen.
- **ausearch -m AVC -ts recent | audit2allow –R**: dieser Befehl gibt Vprschläge, wie die Regeln verbessert werden können, um das Alarmierte zu erlauben

Konfiguration für Syslog Over SSL

Um Syslog over SSL zu verwenden muss bei der entsprechenden Konfigurationsgruppe das Protokoll TCP ausgewählt werden und die Verschlüsselung aktiviert werden, dies geschieht über die Checkbox Verschlüsselung bei der Konfigurationsgruppenänderungsansicht.

Syslog over TLS verschlüsselt den Verkehr zwischen den betroffenen Netzwerkgeräten und dem Proxy.

Syslog over SSL unterstütz die Verschlüsselung des Verkehrs mit Serveridentifizierung. Um sie erfolgreich für den lokalen NetzwerkProxy einzurichten, ist das Zertifikat, welches im Menüpunkt „Log Quellen -> Netzwerk“ heruntergeladen werden kann, notwendig.

In der Konfigurationsgruppenansicht kann, bei aktivierter Verschlüsselung, außerdem die Zertifikatsdatei und die Schlüsseldatei angegeben werden. Sollte Syslog Over SSL beim lokalen NetzwerkProxy verwendet werden, so sind diese beiden Felder leer zu lassen.

Beispiel zum Einrichten von Syslog over SSL auf Linux

Um Linux Syslog over SSL zu versenden, sind die Pakete rsyslog und rsyslog-gnutls notwendig. Diese können über den Paketmanager (yum/apt) installiert werden.

Nach der Installation der Pakete sind in der Datei „/etc/rsyslog.conf“ die Einstellungen zu finden.

Folgende Einstellungen sind für Syslog over SSL wichtig und müssen geändert bzw. ergänzt werden um Clientseitig ohne Überprüfung des Remotehostes zu ermöglichen.

```
$DefaultNetstreamDriverCAFile      /etc/ssl/certs/logapp_syslog_ssl_cert.pem
$DefaultNetstreamDriver            gtls
$ActionSendStreamDriverMode        1
$ActionSendStreamDriverAuthMode    anon
```

Sollte der Hostname mit dem Zertifikat überprüft werden sollen, so sind zum Beipiel diese Einstellungen zu tätigen:

```
$DefaultNetstreamDriverCAFile      /etc/ssl/certs/logapp_syslog_ssl_cert.pem
$DefaultNetstreamDriver            gtls
$ActionSendStreamDriverAuthMode x509/name
$ActionSendStreamDriverPermittedPeer logapp.LAPPDOMAIN
```

Das Zertifikat „logapp_syslog_ssl_cert.pem“ kann von der LogApp im Bereich „LogQuellen“-> Netzwerk heruntergeladen werden.

Als letzte Einstellung ist noch folgendes der Datei „/etc/rsyslog.conf“ im Regelbereich hinzuzufügen:

. @@192.168.80.212:6514

Hierbei handelt es sich um eine Regel, welche alle Logmeldungen mit TCP an die IP Adresse 192.168.80.212 und den Port 6514 sendet.

SyslogRegeln sind im Groben wie folgt aufgebaut:

[facility].[Level] [Protocol][IP]:[Port]

Folgende Werte sind hier zu ergänzen:

- [facility]: Dienst welcher das Log schreibt (z.B. cron, kern, etc.), auf den diese Regel zutreffen soll.
- [Level]: ab diesem Level aufwärts (debug, info, etc.), greift diese Regel.
- [Protocol]: hier wird spezifiziert welches Protokoll verwendet werden soll. @ steht hier für UDP und @@ für TCP
- [IP]: IP auf dem das Empfängergerät die Nachrichten empfangen soll
- [Port]: Port auf dem das Empfängergerät die Nachrichten empfangen soll

Nach den Einstellungen ist noch der Dienst rsyslog durchzustarten. Zum Beispiel mit service rsyslog restart.

Zum Testen kann folgender Befehl verwendet werden:

```
logger "Testnachricht"
```

Sollte die Nachricht nicht versendet werden oder sonstige Probleme auftreten, so können im File /var/log/syslog(Debian/Ubuntu) bzw. /var/log/messages(RHEL/CentOS) die Fehlermeldungen eingesehen werden.

Beispiele für Filter bei Events

Beispiele für Stringfilter bei Events

Alle Stringfelder verwenden Regex mit „Beginnend mit“ als Filteralgorithmus, außerdem ist es möglich mehrere Werte getrennt durch Beistrich zu verwenden. Filtert man nach mehreren Werten, so werden diese mit oder verknüpft.

Daraus ergeben sich eine Vielzahl an Filtermöglichkeiten im Folgenden sind exemplarisch einige aufgelistet:

Anmerkung: In dieser Auflistung wird das Feld Schlüsselwörter verwendet, die angeführten Filter lassen sich jedoch für jedes Stringfeld anwenden. Eine Besonderheit stellen die Filter Raw Message, Nachricht und Beschreibung dar, diese werden anschließend noch genauer behandelt.

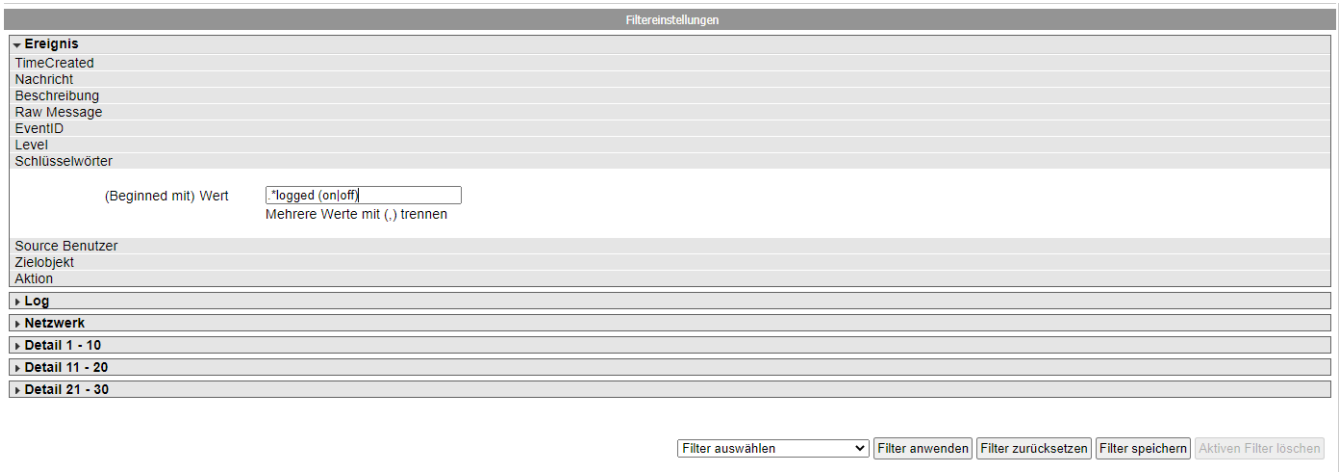

Abbildung 138: Beispiel Filter Ereignisse

Art der Suche	Eingabe	Ergebnis Anmerkung
Übereinstimmung am Beginn	An account	Default-Art der Suche. Kann zu mehrdeutigen Rückmeldungen führen (verschiedene Messages, die mit „An account“ starten (z.B auch „An account was logged off“).
Suche nach ganzer der Message	An account was successfully logged on.	Je länger und exakter die eingegebene Message ist, desto exakter wird das Ergebnis.
Suche nach mehreren Messages	An account was logged off.,An account was successfully logged on.	Ergebnis dieser Suche sind Events, welche mit „An account was logged off.“ Oder „An account was successfully logged on.“ Beginnen.
Volltextsuche	.*successfully	Der Suchstring kann an beliebiger Stelle vorkommen.
Suche mit Regex	(L|l)ogin	Suche nach allen Message, die mit Login oder login starten

Suche mit Regex	.*(Process|Prozess)	Volltextsuche, bei dem Process oder Prozess an beliebiger Stelle vorkommen können

Tabelle 40: Beispiele für Stringfilter bei Ereignissen

Fulltext filter (Bachricht, Beschreibung und Raw Message)

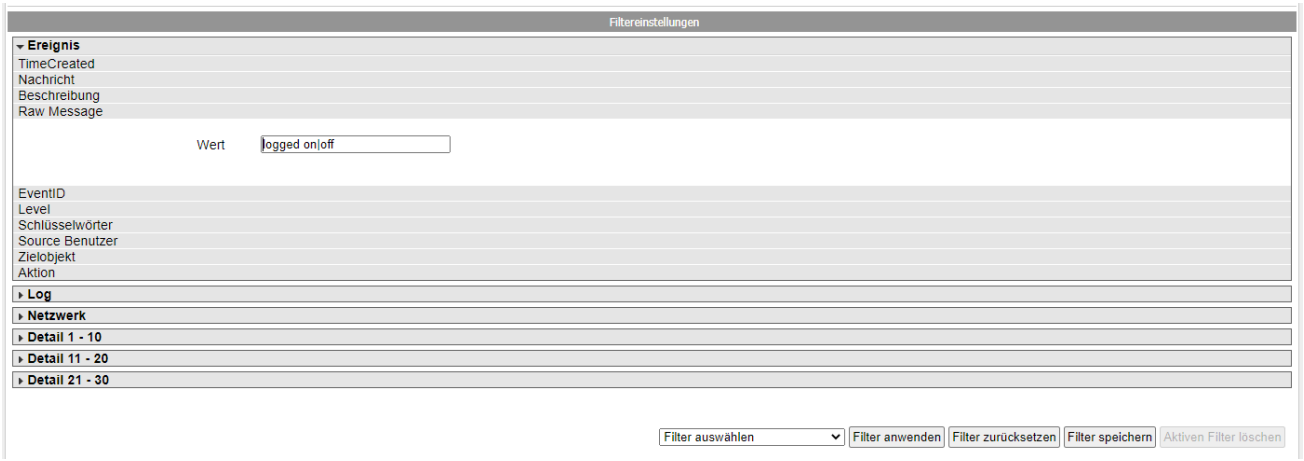

Abbildung 139: Beispiel Filter Raw Message

Die Suche folgt, im Gegensatz zu allen anderen StringFeldern, dem Algorithmus der **Volltextsuche (Suche an beliebiger Stelle)**.

Wird in der Raw Message gesucht ist es zusätzlich noch zu empfehlen das Suchergebniss vorher einzuschränken (z.B. mit einem Datumsfilter).

Bei der Volltextsuche können verschiedene Wildcards eingesetzt werden:

Zeichen	Beschreibung
+	Und – Operator (&& erreicht das gleiche)
|	Oder - Operator
*	Wildcard. Steht für eine beliebig Anzahl beliebiger Zeichen
„“	Phrase (Suche nach exakt dieser Phrase)
-	Negierung (ein ! erreicht das gleiche)
( )	Definiert eine logische Gruppe um Abfragen wie (admin | Admin) + logout zu ermöglichen
?	Wildcard, welches für ein einzelnes Zeichen steht
/	Wird verwendet um eine Regex anzugeben (/RegEx/)

Tabelle 41: Wildcards bei Fulltextfiltern

Reservierte Zeichen

Beim Filtern mit einem Fulltextfilter sind gewisse Zeichen reserviert und müssen dementsprechend mit \ escaped werden. Diese Zeichen sind +, -, =, &&, ||, >, <, !, (,), {, }, [,], ^, ", ~, *, ?, :, \, /.

Art der Suche	Eingabe	Ergebnis Anmerkung
Volltextsuche	LADemo	Default-Art der Suche. Liefert alle Events, welche an beliebiger Stelle den Term LADemo enthalten.
Volltextsuche in Windows Events	'TargetUserSid'>S-1-5-18	Um einen Wert in einem konkreten XML-Tag abzufragen, sollte der führende Tag mitangeführt werden.
Such nach mehreren möglichen Werten	Login Logon	Diese Suche liefert Ereignisse zurück, welche im betroffenen Feld Login oder Logon oder beides haben zurück.
Suche nach Phrase	„Successfull Logon“.	Ergebnis dieser Suche sind Events, welche in der Raw Message exact Successfull Logon aufweisen
Suche mit WIldcard	(L|l)ogin	Suche nach allen Events, in deren RawMessage Login oder login vorkommen
Suche mit Wildcard	Log*	Volltextsuche nach Events in denen ein Term zu finden ist, der mit Log beginnt
Suche mit Wildcard	Successfull+Logon	Volltextsuche, bei dem die Terms Successfull und Logon vorkommen müssen, diese müssen jedoch nicht in dieser Reihenfolge und auch nicht hintereinander vorkommen.
Suche mit Wildcard	-admin login	Suche nach Events in denen der Term login vorkommt aber nicht der Term admin

Tabelle 42: Beispiele für Fulltext Filtern bei Ereignissen

Beispiele für Zahlenwertfilter bei Events

In allen Zahlenfiltern können sowohl einzelne Zahlen als auch Bereiche gefiltert werden. Bereiche werden dabei getrennt von – angegeben (z.B. 102-1000). Eine weitere Möglichkeit besteht mit der Checkbox Ungleich, mit der sich das Ergebnis negieren lässt, so liefert der Filter als Ergebnis des Wertes 102 (Ungleich) in der EventID alle Ereignisse welch nicht die EventID 102 haben.

Abbildung 140: Beispiel Filter Zahlenwert Event

Beispiel:

Für die Beispiele wird der Filter EventID verwendet

Art der Suche	Eingabe	Ergebnis Anmerkung
Einzelwertsuche	102	Liefert alle Ereignisse mit EventID 102
Negierte Enzelwertsuche	102 (Ungleich Checkbox aktiviert)	Liefert alle Ereignisse, welche eine andere EventID haben als 102 (Ereignisse welche keine EventID haben werden ebenfalls zurückgeliefert)
Bereichssuche	102-1000	Liefert Ereignisse, welche eine EventID aufweisen, die zwischen 102 und 1000 liegt (einschließlich der Grenzen 102 und 1000)
Negierte Bereichssuche	102-1000 (Ungleich Checkbox aktiviert)	Liefert Ereignisse, welche nicht eine EventID aufweisen, die zwischen 102 und 1000 liegt (einschließlich der Grenzen 102 und 1000)

Tabelle 43: Beispiele für Zahlenwertfilter

Stringfilter für Alarme

Der Stingfilter ist mit dem Algorithmus “Beginned mit“ implementiert.

Als Wildcard dient %. Es können mehrere Werte getrennt durch „ , “ gefiltert werden.

Die Wildcard % steht für beliebig viele Zeichen jedweder Art.

Beispiele:

Für die Beispiele wird das Feld „Alarm Name verwendet“.

Art der Suche	Eingabe	Ergebnis Anmerkung
Übereinstimmung am Beginn	[Windows Security]	Default-Art der Suche. Kann zu mehrdeutigen Rückmeldungen führen (verschiedene Alarme, welche mit [Windows Security] beginnen, z.B. „[Windows Security] Logon/Logof“ oder „[Windows Security] Poilicy Change“).
Suche nach der ganzen Message	[Windows Security] Logon/Logoff	Je länger und exakter der eingegebene Alarmname ist, desto exakter wird das Ergebnis.
Suche nach mehreren Messages	[Windows Security],[Change Auditing]	Ergebnis dieser Suche sind Alarme, welche mit [Windows Security] oder [Change Auditing] beginnen.
Volltextsuche	%Logon	Als Ergebnis werden Alarme geliefert welche an beliebiger Stelle die Zeichenkette „Logon“ im Alarmnamen aufweisen.

Tabelle 44: Beispiele Stringfilter Alarme

Entsperren eines Index

Sollte zu wenig Platz auf der Festplatte verfügbar sein und die Festplatte wurde nicht rechtzeitig erweitert, so kann es sein, dass ein Index gesperrt wurde. Wird die Festplatte nun erweitert, so muss der Index wieder entsperrt werden. Dies geschieht mit folgendem Befehl im Supportmodus:

```
/usr/sbin/LogAppScripts/Elasticsearch/undoReadonlySettingForEsIndex.bash --
indexname logappclient1_2022_12_09*
```

Beim parameter –indexname kann wie bei anderen IndexingEngine Befehlen eine Wildcard in Form von * verwendet werden.

Abbildungsverzeichnis

Tabellenverzeichnis