NEWS-LETTER

2024/1

Zu gewinnen: Blumen-Abo

Wie wir mit neuer, ganzheitlicher Logtechnik all das überblicken, registrieren, analysieren und verstehen, was mit Ihren Systemen passiert – und das 24/7. Welche neuen Projekte wir anpacken, mit welchen Profis wir uns dafür verstärkt haben. Dieser Newsletter informiert kompakt und illustriert.

aspectra AG
Weberstrasse 4
8004 Zürich
Tel. +41 44 296 56 56
info@aspectra.ch

www.aspectra.ch
twitter.com/aspectra
linkedin.com/company/aspectra-ag
xing.com/companies/aspectraag

Impressum Redaktion: Norbert Benz und Edina Gallos / Realisation und Gestaltung: Bernet Relations und Frau Schmid / Druck: rb druck AG
Kontakt, Zusatzbestellungen sowie Abmeldung: +41 44 296 56 56 oder info@aspectra.ch

Für leichtere Lesbarkeit verwenden wir im Newsletter die männliche Sprachform bei personenbezogenen Substantiven und Pronomen. Dies soll im Sinne der sprachlichen Vereinfachung als geschlechtsneutral zu verstehen sein.

aspectra
hosting your future

EDITORIAL

LIEBE LESERIN, LIEBER LESER

24/7 strömen Logfiles aus Ihren Systemen und Applikationen – was passiert damit und was lernen wir daraus? Wir wollen Ereignisse, Prozesse und Transaktionen auf allen von aspectra gemanagten Systemen jederzeit erkennen, verstehen und analysieren. Das hilft uns beim Risikomanagement und der Früherkennung von Fehlern oder Angriffen. Mit dem aspectra Central Log Monitoring und Management haben wir ein ganzheitliches System auf einer modernen Plattform geschaffen. Sie überwacht und verwaltet Daten und Systeme sicher und zentral. Mehr dazu auf der Rückseite.

Zudem erfahren Sie, welche spannenden Kundenprojekte wir neu begleiten und umsetzen (nur jene, die wir nennen dürfen) und wie wir Kundenanliegen zukünftig noch schneller bearbeiten. Dafür haben wir uns verstärkt: Zwölf neue Kolleginnen und Kollegen arbeiten zusätzlich für unsere Projekte und sorgen für ein hochsicheres Hosting und Top-Performance aller Applikationen. Sie werden diesen Ideen- und Energieschub auch zu spüren bekommen – davon sind wir überzeugt.

Good News gibt es auch für Wissenshungrige, die immer gerne unsere Business-Breakfasts besuchen.

Kein aspectra-Newsletter ohne Gewinn – von Infos und «gifts that keep giving». Diesmal wollen wir Sie mit einem Blumen-Abo im Wert von CHF 1000 begeistern. Wir wünschen viel Glück und eine inspirierende Lektüre.

Auf bald!

aspectra AG
Kaspar Geiser und Norbert Benz

NEWS

NEUE KUNDENPROJEKTE

Medizinische Daten sind besonders sensibel und erfordern einen verantwortungsvollen und sicheren Umgang. Umso mehr freuen wir uns über das entgegengebrachte Vertrauen eines Anbieters, der **Lösungen für den Austausch medizinischer Daten** bereitstellt. Wir hosten seine Produktionsumgebung und stellen sicher, dass die neuesten Versionen von Software, Produkten und/oder Updates live an die vorgesehenen Benutzer übertragen werden.

Weiter sind wir seit Kurzem für die **Infrastruktur und die geschäftskritischen Anwendungen** der wichtigsten Schweizer Organisation für Personen- und Fahrzeug-Assistance zuständig.

Unsere **Akamai-WAF-Projekte** haben sich gut entwickelt und laufend Zuwachs bekommen. Ebenso konnten wir diverse Neukunden von unserem **WAF und IAM as a Service** auf der Basis des Airlock Secure Access Hub überzeugen.

VERBESSERTE ABLÄUFE UND SERVICES

Neue Projekte zu gewinnen ist toll und motivierend. Wir wollen aber auch unsere vielen langjährigen Kunden immer wieder von Neuem von unseren Qualitäten überzeugen. Darum bearbeiten wir Ihre Anliegen nun noch schneller. **Wenn es «brennt», zählt jede Sekunde.** Ihr Ticket gelangt auf direktem Weg an die richtige Person, die es effizient bearbeitet. Die Reaktionszeit ist spürbar kürzer.

Und weitere Optimierungen sind in Sichtweite: Erste neue Logkonsolen sind im Frühjahr für Kunden verfügbar.

NEUES AUS DEM HR

Gut ein Dutzend neue Kolleginnen und Kollegen sind im vergangenen Jahr zu uns gestossen und setzen ihr Know-how für Kundenlösungen ein, **bringen frische Ideen und sorgen für einen Energieschub** in den Teams. Diese gewonnene Energie ist für uns sehr wertvoll, da wir stetig neue Projekte umsetzen dürfen. Unsere Suche nach kompetenten Fachpersonen ist noch nicht abgeschlossen. Wir freuen uns auf weitere Kolleginnen und Kollegen.

Zum **«Hallo»** gehört oft auch **«Adieu».** Letztes Jahr zog es einige unserer langjährigen und geschätzten Mitarbeitenden in andere Gefilde. Wir wünschen viel Erfolg und freuen uns, wenn sie ihr grosses Fachwissen weiter nutzen.

Interessiert an einer Karriere bei aspectra mit spannenden Projekten, anspruchsvollen Kunden und kompetenten Kollegen?

Aktuelle Stellen:
karriere.aspectra.ch

DIE ZAHL

1000 ZEILEN PRO SEKUNDE

Das ist der durchschnittliche Input, den unser Log Collector von den angeschlossenen Endpoints – einschliesslich Kunden- und aspectra-Basissystemen – und leitet sie sicher an die Rule Transformer Engine weiter. Das sind bis zu 2 TB pro Tag!

EVENTS

Auch 2024 stehen wir früh auf für Wissenshungrige und setzen die Frühstücksreihe «IT for Breakfast» fort. Interessierte tauchen in unsere Technologien und Lösungen ein und dürfen sich auf Expertenwissen und anschauliche Praxisbeispiele freuen. Den Auftakt machen wir am Mittwoch, 8. Mai 2024 mit dem Schwergewicht **OpenShift – Verfügbarkeit, CI/CD und mehr.**

WETTBEWERB

VON WELCHER KOMPONENTE DES LOG-PROZESSORS WIRD GESTEUERT, WIE LANGE DIE DATEIEN AUFBEWAHRT WERDEN?

Unter den Teilnehmenden verlosen wir ein Abo von Tom Flowers im Wert von CHF 1000 für regelmässig frische und saisonale Blumensträusse an eine CH-Wunschadresse.

Antwort bis zum 31. März 2024 an info@aspectra.ch. Die Gewinnerin oder der Gewinner wird von uns persönlich benachrichtigt.

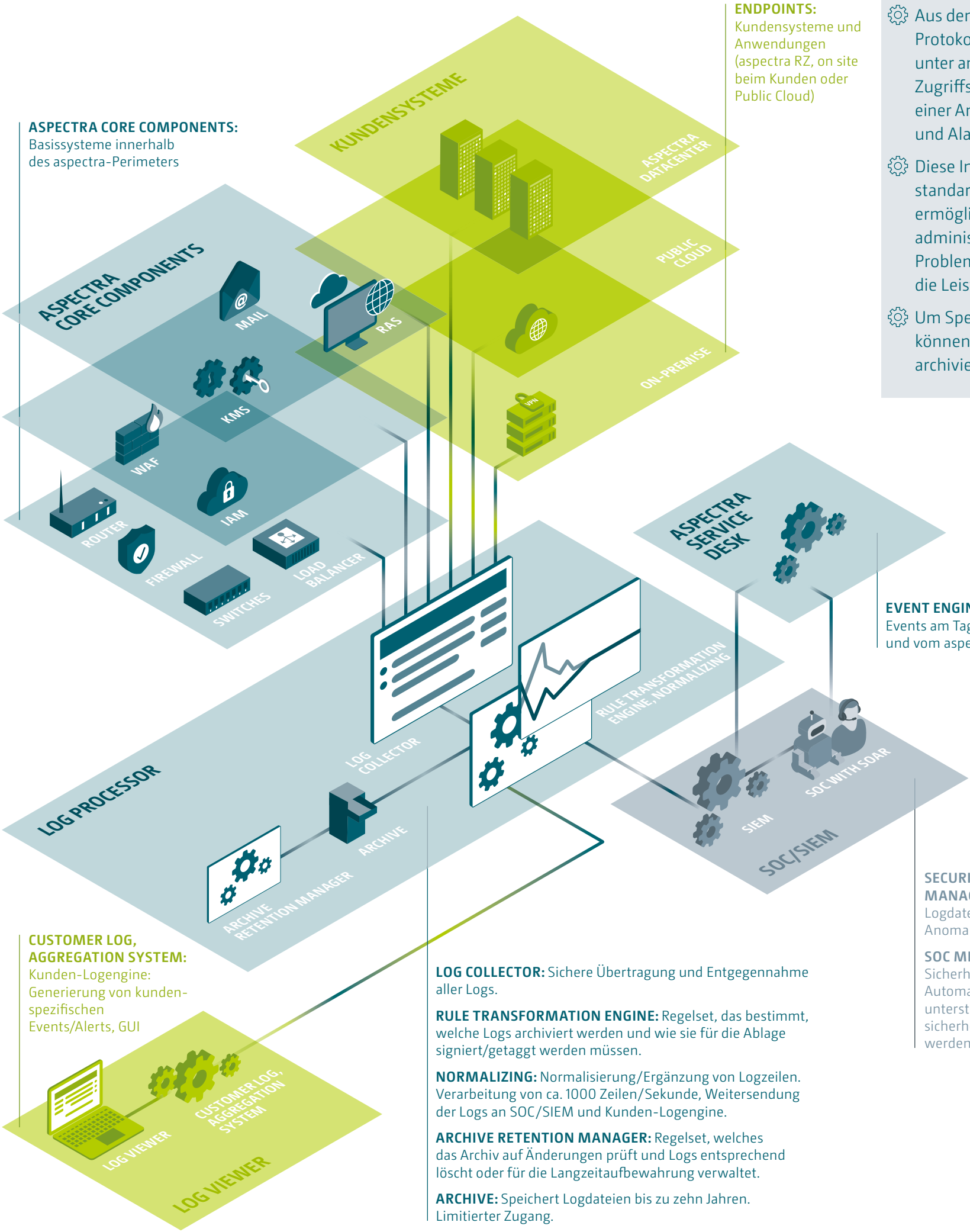
DAS ASPECTRA LOGUNIVERSUM: EINE PLATTFORM ZUR ÜBERWACHUNG UND VERWALTUNG VON PROTOKOLLDATEIEN

Logfiles sind das zentrale Instrument zur Problemanalyse. Sie zeichnen alles auf, was in der Applikation, im System und im Netzwerk ausgeführt wird und auftritt. Das Central Log sorgt dafür, dass diese grossen Mengen an Logdaten aus unterschiedlichen Quellen effizient verarbeitet, archiviert und analysiert werden können.

Uns von aspectra gefällt moderne Architektur – auch in der IT. Sie skaliert besser, bringt die Daten in «einen Guss» und ermöglicht eine Analyse, die übersichtliche und schnell interpretierbare Dashboards liefert. Das unterstützt ein unmittelbares Risikomanagement und eine proaktive Fehlererkennung und -behebung.

WAS SIND LOGDATEIEN?

- Logdateien werden von jeder Netzwerkkomponente automatisch generiert und zeichnen Details von Ereignissen und Aktivitäten lückenlos und nachvollziehbar auf.
- Jeder Logeintrag enthält Informationen zu einem Ereignis und zum Zeitpunkt des Auftretens.
- Aus den Logdateien werden detaillierte Protokolle erstellt. Dazu gehören unter anderem Systemstarts und -stopps, Zugriffsversuche, Änderungen an einer Anwendung oder Datei sowie Fehler- und Alarmmeldungen.
- Diese Informationen werden aggregiert, standardisiert und normalisiert und ermöglichen es Entwicklern, Systemadministratoren und Support-Teams, Probleme zu erkennen, zu lösen und die Leistung zu überwachen.
- Um Speicherplatz zu sparen, können Logdateien komprimiert und archiviert werden.



ENDPOINTS: Kundensysteme und Anwendungen (aspectra RZ, on site beim Kunden oder Public Cloud)

ASPECTRA CORE COMPONENTS: Basissysteme innerhalb des aspectra-Perimeters

EVENT ENGINE / EVENT ALERTS: Bis zu zehn Events am Tag werden aus dem SIEM generiert und vom aspectra-Servicedesk bearbeitet.

SECURITY INFORMATION AND EVENT MANAGEMENT SYSTEM: Die zentrale Stelle, die Logdaten sammelt und korreliert. Hier werden Anomalien entdeckt und daraus Events generiert.

SOC MIT SOAR: Security Operation Center, dessen Sicherheitsteam durch eine «Security Orchestration, Automation and Response (SOAR)»-Plattform unterstützt wird. Hier können aus der Datenflut sicherheitsrelevante Anomalien herausgefiltert werden.

CUSTOMER LOG, AGGREGATION SYSTEM: Kunden-Logengine: Generierung von kundenspezifischen Events/Alerts, GUI

LOG COLLECTOR: Sichere Übertragung und Entgegennahme aller Logs.

RULE TRANSFORMATION ENGINE: Regelset, das bestimmt, welche Logs archiviert werden und wie sie für die Ablage signiert/getaggt werden müssen.

NORMALIZING: Normalisierung/Ergänzung von Logzeilen. Verarbeitung von ca. 1000 Zeilen/Sekunde, Weitersendung der Logs an SOC/SIEM und Kunden-Logengine.

ARCHIVE RETENTION MANAGER: Regelset, welches das Archiv auf Änderungen prüft und Logs entsprechend löscht oder für die Langzeitaufbewahrung verwaltet.

ARCHIVE: Speichert Logdateien bis zu zehn Jahren. Limitierter Zugang.

aspectra
hosting your future