



FARONICS™ Cloud

Überblick über Architektur und Sicherheit

Einführung

Faronics Cloud bezieht sich auf Faronics Cloud Deep Freeze und Faronics Cloud Deploy (im Folgenden als „Faronics Cloud“ bezeichnet).

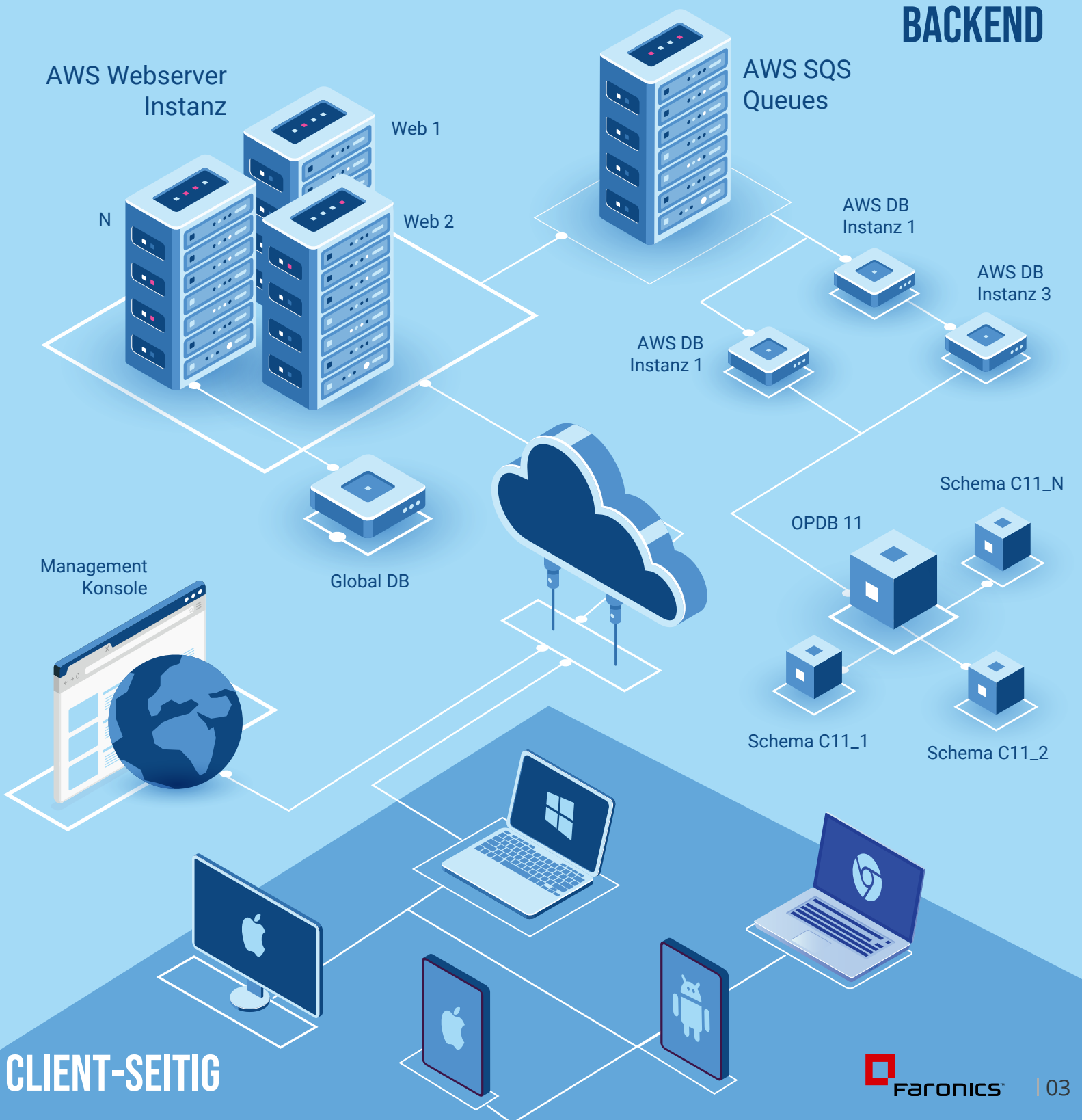
Faronics Cloud ist eine einheitliche Plattform, die es Kunden ermöglicht, die Verwaltung ihrer Endpunkte über das Internet zu vereinfachen. Sie umfasst eine breite Palette an Services, wie z. B. PC- und Mac-Verwaltung, die Verwaltung mobiler Geräte, Antivirus, Anwendungs-Whitelisting, Datenschutz, Asset-Verwaltung, Energieverwaltung und mehr.

Dieses Dokument bietet einen umfassenden Überblick über die Cloud-Architektur von Faronics. Es beschreibt, wie die Sicherheit und der Datenschutz der Kundendaten von allen Parteien im Rahmen des Modells der geteilten Verantwortung geschützt werden. Dieses Dokument erläutert auch die Sicherheitsrichtlinien, -prozesse und -praktiken, die das Faronics-Team befolgt, um seiner eigenen Verantwortung für die Sicherheit der Faronics Cloud nachzukommen.



Überblick über die Architektur

Die Faronics Cloud besteht aus zwei großen Teilen: Client-seitigen Komponenten und Backend-Komponenten.



Client-seitige Komponenten

Jeder verwaltete Computer (Client) enthält einen Cloud Agent und verschiedene Services, wie in den Richtlinieneinstellungen des Clients festgelegt. Für bestimmte Services kann der Kunde optional einen Cache-Server-Computer in seinem lokalen Netzwerk einrichten, um Bandbreite zu sparen. Systemadministratoren greifen über ihren Internetbrowser auf die Verwaltungskonsolle zu.

Backend-Komponenten

Die Backend-Komponenten der Faronics Cloud werden auf Amazon Web Services (AWS) gehostet. Die Produktionsumgebung wird in zwei AWS-Regionen gehostet: US West (Oregon) und EU (Irland). Die Backup-Replikationsumgebung wird in zwei AWS-Regionen gehostet: US East (N. Virginia) und EU (Frankfurt) für das Disaster Recovery. Eine Farm von Webservern empfängt und beantwortet alle Anfragen von verwalteten Clients und Cloud-Konsolen. Sie leiten außerdem Anfragen über den AWS Simple Queue Service (SQS) zur Verarbeitung an den Datenbankserver weiter. Eine globale Datenbank, die auf AWS Multi-AZ RDS-Instanzen gehostet wird, speichert global erforderliche Systemdaten. Eine separate Datenbank enthält die isolierten Datenbankschemata, die für jeden Kunden erstellt wurden.

Faronics Cloud-Sicherheit und Datenschutz

Informationssicherheit und Datenschutz für unsere Kunden sind für uns bei Faronics von größter Wichtigkeit. Indem wir die branchenweit bewährten Sicherheitspraktiken befolgen, möchte Faronics Kundendaten und Privatsphäre vor versehentlichem oder vorsätzlichem Diebstahl, Datenlecks, Integritätsbeeinträchtigungen und Hackern schützen.

Das Modell der geteilten Verantwortung

Da es sich um eine Cloud-Lösung handelt, teilen sich AWS (der Cloud-Service-Anbieter von Faronics Cloud), Faronics (der Cloud-Service-Anbieter für die Kunden) und Kunden von Faronics Cloud die Verantwortung für die Datensicherheit.

Die AWS-Infrastruktur und -Services erfüllen mehrere branchenspezifische Standards, einschließlich:



Cloud Security Alliance
(CSA)



HIPAA



Motion Picture Association
of America (MPAA)



AWS INFRASTRUKTUR UND SERVICES

AWS stellt detaillierte Informationen zur IT-Kontrollumgebung durch Whitepapers, Berichte, Zertifizierungen, Akkreditierungen und andere Bescheinigungen Dritter bereit. Weitere Informationen finden Sie im Whitepaper zum Thema Risiko und Compliance auf der Website. <http://aws.amazon.com/security>.

Faronics ist für die Sicherheit des Backend-Betriebssystems, des Netzwerks, der Firewall-Konfigurationen, der Plattform- und Anwendungsverwaltung sowie der Kundendaten verantwortlich. Unsere Sicherheitsrichtlinien und -praktiken werden unten in den Abschnitten Kundendaten und Datenschutz sowie Sicherheitsrichtlinien und -praktiken beschrieben.

Kunden von Faronics Cloud sind für ihre eigene Datensicherheit verantwortlich. Sie müssen den Zugriff und die Berechtigungen für ihre Konten bei Faronics Cloud verwalten, ihre Anmeldedaten sicher aufbewahren und sichere Kennwörter verwenden.

Kundendaten und Datenschutz

Gesammelte Kundendaten

Faronics only collects personal information for the following reasons:

- Um unsere Produkte und Services für unsere Kunden zu entwickeln, zu verwalten und zu liefern.
- Um Kunden wegen Produkt- und Service-Updates, -Upgrades und -Verbesserungen zu kontaktieren.
- Um unsere Kunden entweder direkt oder über einen unserer Wiederverkäufer zu kontaktieren, um ihnen die Möglichkeit zu bieten, Services zu erneuern.
- Um unsere Kunden direkt über Produkte und Services zu informieren, die für sie von Interesse sein könnten.
- Um unseren Kunden hohe Servicestandards zu gewährleisten.
- Um die Identität eines Kunden zu verifizieren.
- Um regulatorische Anforderungen zu erfüllen.

Im Faronics Cloud-System können je nach den vom Kunden genutzten Services folgende Kundendaten gesammelt werden:

- Kundenidentität und Kontoinformationen, einschließlich Organisationsname, Benutzername, Kennwort, Titel, Telefonnummer, E-Mail-Adresse und ähnliches.
- Informationen zum Gerät des Kunden, einschließlich Gerätename, IP-Adresse, MAC-Adresse, Datum/Uhrzeit der Verbindung mit dem Faronics Cloud-Server und ähnliches.
- Informationen zur Gerätenutzung durch den Kunden, einschließlich Datum/Uhrzeit der Benutzeranmeldung/-abmeldung, auf dem Gerät installierte Software, Softwarenutzung auf dem Gerät und ähnliches.
- Konfigurationen und Auswahlmöglichkeiten für den Faronics Cloud-Service

Segmentierung von Kundendaten

Faronics Cloud segmentiert Kundendaten (einschließlich Gerätedetails, aber keine personenbezogenen Daten) in dedizierte Datenbankschemata, in denen alle Tabellen einem bestimmten Kunden gehören. Jedes kundenspezifische Datenbankschemata wird auf einer geteilten Datenbankinstanz in AWS gehostet. Die Architektur ist ausreichend flexibel, sodass Kunden eine dedizierte Datenbankinstanz für ihre Daten anfordern können. Beachten Sie, dass für die Datentrennung zusätzliche Kosten für den Kunden anfallen können.

Schutz von Kundendaten während der Übermittlung

Die Faronics Cloud-Server nutzen die HTTPS-(TLS 1.2)-Verschlüsselung. Faronics verschlüsselt vertrauliche Kundendaten im Ruhezustand, wie z. B. Kennwörter, Richtlinien und Strings für die Datenbankverbindung, je nach Datentyp:

- Kennwort-Hashes verwenden eine Einwegverschlüsselung.
- Strings für die Datenbankverbindung werden mit einem 256-Bit-Rijndael-Algorithmus verschlüsselt.
- Richtlinien werden abhängig vom jeweiligen Service mit einem RC4-Stream-Verschlüsselungsalgorithmus verschlüsselt, der vom Microsoft Base Cryptographic Provider unterstützt wird.

Schutz von gespeicherten Kundendaten

Die Backup-Daten der Faronics Cloud werden im AWS mit aktivierter Verschlüsselung gespeichert. Vertrauliche Daten werden immer vorverschlüsselt.



Sicherheitsrichtlinien und -praktiken

Sicherheitsrichtlinien und -praktiken für Entwicklung und Qualitätssicherung

Die Entwicklungs- und Qualitätssicherungsprozesse von Faronics werden unter Berücksichtigung von Sicherheitsrisiken und Schwachstellen konzipiert. Zu den relevanten Best Practices gehören unter anderem die Folgenden:

- Quellcode-Builds werden auf Malware gescannt und der gesamte Sicherheitscode wird vor der Bereitstellung überprüft.
- Das Entwicklungsteam führt regelmäßig Penetrationstests auf Anwendungsebene durch, wie es in den branchenüblichen Best Practices und Leitlinien vorgeschrieben ist. Das Team für den Betrieb testet die Geschäftskontinuitäts- und
- Disaster-Recovery-Pläne für kritische Services gemäß einem definierten Testplan und für verschiedene Verlustszenarien.
- Vor der Bereitstellung werden für alle Versionen Sicherheitstests durchgeführt.
- Kontinuierliche Sicherheitsverbesserung innerhalb des System-/Softwareentwicklungslebenszyklus (System/Software Development Lifecycle, SDLC) mithilfe der Sicherheitsmaßnahmen Prevent Breach und Assume Breach.

Faronics hat Softwareentwicklungs- und Release-Management-Prozesse etabliert, um die Umsetzung wichtiger Änderungen zu steuern, darunter unter anderem:

- Geplante Änderungen werden identifiziert und dokumentiert, einschließlich der Erstellung von Funktionsspezifikationen und Komponentendesigns.
- Geschäftsziele, Prioritäten und Szenarien werden während der Produktplanung identifiziert.
- Die Einsatzbereitschaft wird gemäß vordefinierter Kriterien überprüft und das Gesamtrisiko und die Auswirkungen werden bewertet.
- Tests, Autorisierung und Änderungsmanagement basierend auf Ein- und Ausstiegsriterien für DEV- (Entwicklung), INT- (Integrationstests), STAGE- (Vorproduktion) und PROD-(Produktion)-Umgebungen, wie jeweils anwendbar.
- Faronics gewährleistet die Bereinigung von Datenbankeingaben und Benutzereingaben mithilfe der folgenden bewährten Verfahren:
 - Eingaben werden durch eine grundlegende Validierung.
 - die ordnungsgemäße Verwendung von .NET SqlCommand und SqlParameter eingeschränkt.
 - SQL-Abfragen werden niemals direkt manipuliert oder verkettet.

Richtlinien und Praktiken zur Betriebssicherheit

Da wir die branchenweit bewährten Sicherheitspraktiken befolgen, ist der Betrieb der Faronics Cloud darauf ausgelegt, einen robusten Schutz und Datenschutz für Kundendaten zu bieten. Relevante Richtlinien sind unter anderem die Folgenden:

- AWS IAM (Identity and Access Management): Dieser Service wird für das Authentifizierungsmanagement für Benutzer, Gruppen und Rollen in der Backend-Umgebung genutzt.
- AWS VPC (Virtual Private Cloud), Network ACL (Access Control List) und Security Group: Sie werden zum Schutz der Backend-Infrastruktur (EC2-Instanzen und RDS-Instanz) verwendet.
- Aktivitäten auf der AWS-Plattform werden mit der AWS CloudTrail geprüft.
- Änderungen an der Produktions-Site der Faronics Cloud werden in Übereinstimmung mit den Richtlinien im Änderungsmanagementdokument vorgenommen.
- Komponenten und Prozesse werden mit den minimalen Benutzerrechten ausgestattet, die zur Erfüllung der Aufgaben erforderlich sind.
- Autorisiertes internes Personal bei Faronics mit Zugriff auf Kundendaten im Faronics Cloud-Service muss die MFA-Anmeldung (Multi-Faktor-Authentifizierung) verwenden.
- Die Systeminfrastruktur ist für Redundanz und eine reibungslose Failover-Abwicklung konfiguriert.

- Die Daten werden regelmäßig gesichert und Backups werden in regelmäßigen Abständen für die Wiederherstellung zu Zwecken der Disaster Recovery validiert. Backup-Standards, -Richtlinien, -Verfahren und -Kontrollen werden überprüft und dokumentiert.
 - Cloud-Services können im Falle eines Stromausfalls im Rechenzentrum, eines Netzwerkausfalls oder in anderen Katastrophensituationen in einer anderen Verfügbarkeitszone innerhalb derselben AWS-Region oder in verschiedenen AWS-Regionen wiederhergestellt werden. Wiederherstellungsprozesse werden definiert und dokumentiert
- Der Betrieb unterliegt regelmäßigen internen Sicherheitsaudits auf der Grundlage von Traces, Protokollen und anderen Informationen, die von Systemadministratoren und anderen am Routinebetrieb beteiligten Parteien durchgeführt werden.

References and further reading

[AWS-Standard für bewährte Sicherheitsverfahren \(von Amazon Web Service\)](#)

[Treacherous 12 Top Threat to Cloud Computing Plus: Industry Insights \(von Cloud Security Alliance \(CA\)\)](#)

[OWASP Top 10 2017 - The Ten Most Critical Web Application Security Risks](#)

HINWEIS: Dieses Dokument dient nur zu Informationszwecken. Es stellt die aktuellen Produktangebote und -praktiken von Faronics zum Zeitpunkt der Veröffentlichung dieses Dokuments dar und kann ohne Vorankündigung geändert werden. Kunden sind dafür verantwortlich, ihre eigene unabhängige Bewertung der Informationen in diesem Dokument und jeglicher Nutzung der Produkte und Services von Faronics vorzunehmen, die jeweils „wie gesehen“ ohne Gewährleistung jeglicher Art, sei sie ausdrücklich oder stillschweigend, bereitgestellt werden. Dieses Dokument begründet keine Garantien, Zusicherungen, vertraglichen Verpflichtungen, Bedingungen oder Versicherungen vonseiten von Faronics, seinen verbundenen Unternehmen, Lieferanten oder Lizenzgebern. Die Verantwortlichkeiten und Verbindlichkeiten von Faronics gegenüber seinen Kunden werden durch Faronics-Vereinbarungen geregelt. Dieses Dokument ist weder Teil einer Vereinbarung zwischen Faronics und seinen Kunden, noch ändert es sie.



Damit wir Ihnen zeigen können, wie Ihre Rechnerumgebungen von den Lösungen von Faronics profitieren können, besuchen Sie uns unter www.faronics.com

UNITED STATES

5506 Sunol Blvd, Suite 202
Pleasanton, CA, 94566 USA

Gebührenfreie Rufnummer:
1-800-943-6422
Faxnummer: 1-800-943-6488

sales@faronics.com

EUROPA

8 The Courtyard, Eastern Road,
Bracknell, Berkshire
RG12 2XB, United Kingdom

Telefon: +44 (0) 1344 206 414

eurosales@faronics.com

KANADA/INTERNATIONAL

609 Granville Street, Suite 1400
P.O. Box 10362, Pacific Centre
Vancouver, BC, V7Y 1G5

Telefon: +1-604-637-3333
Fax: +1-604-637-8188

sales@faronics.com

SINGAPUR

6 Marina Boulevard
#36-22 The Sail At Marina Bay
Singapore, 018985

Telefon: +65 6509 4993
Fax: +65 6722 8634

sales@faronics.com.sg