alessa

ÜBERBLICK ÜBER DIE SYSTEMARCHITEKTUR

VERSION 5

CaseWare

CaseWare RCM ist ein weltweiter Anbieter von Unternehmenssoftwarelösungen, die sich mit Wirtschaftskriminalität, Risiko und Compliance befassen. Unsere Technologielösungen werden in mehr als 20 Ländern von Fortune 500- und Global 500-Unternehmen in den Bereichen Banken, Finanzen, Einzelhandel, Fertigung, Gesundheitswesen und von Regierungsbehörden zur Echtzeit-Überprüfung und -Überwachung von Transaktionen, zur Ermittlung von Geldwäsche, zur Kenne-Deinen-Kunden-Compliance (KYC), zur Überprüfung von Sanktionslisten, für das Meldungswesen, zur Fall- und Workflow-Verwaltung sowie zur kontinuierlichen Überprüfung von Kontrollen innerhalb einer einzigen Plattform eingesetzt. Weitere Informationen finden Sie unter alessa.caseware.com.

Alessa ist ein exklusives Lizenzprodukt von:

CaseWare RCM Inc.
1 Toronto Street, Suite 1400
Toronto ON M5C 2V6
CANADA

Inhaltsverzeichnis

Überblick

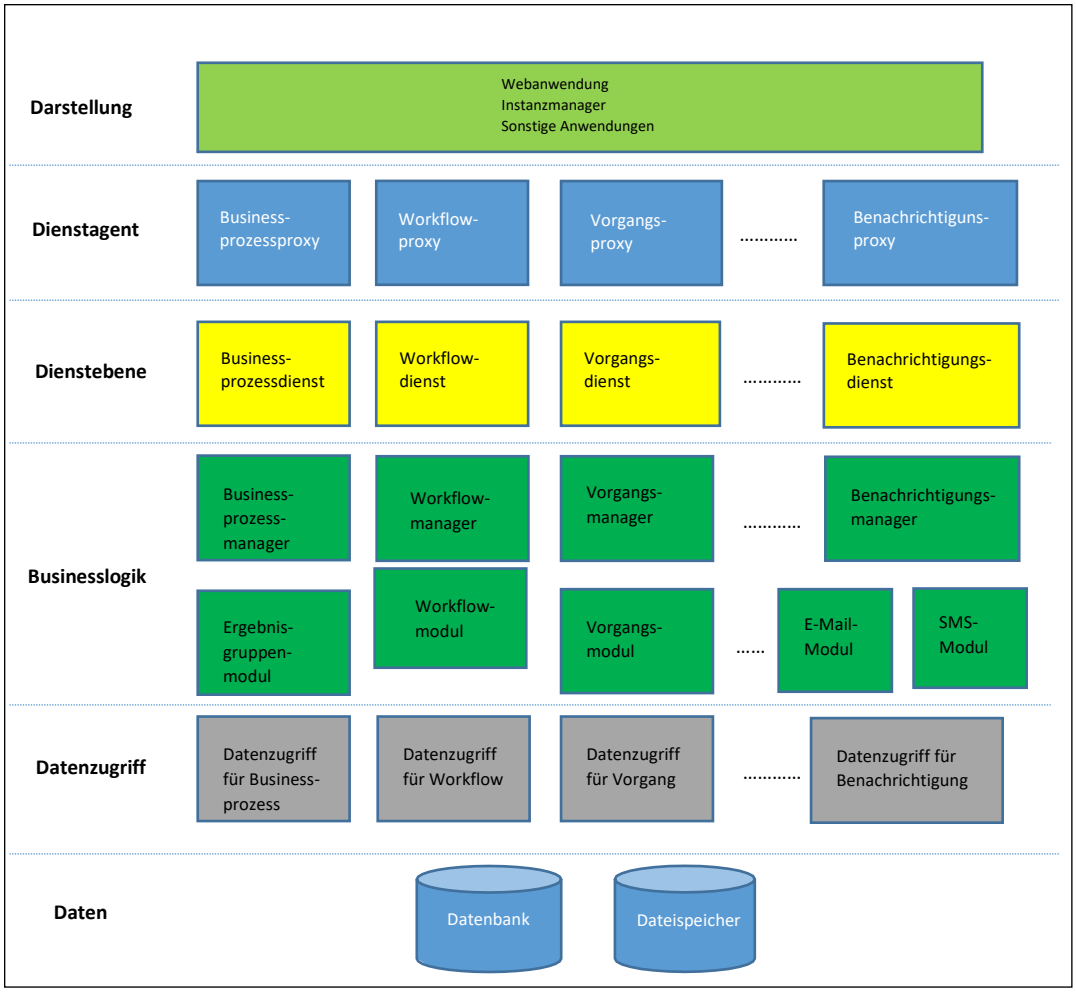
Das vorliegende Dokument bietet einen Überblick über die Systemarchitektur von Alessa. Es ist für IT-Spezialisten vorgesehen, die für die Installation, Konfiguration und die Pflege der Anwendung verantwortlich sind.

Einführung

Alessa basiert auf der Microsoft .NET-Plattform und besteht aus den folgenden Softwarekomponenten:

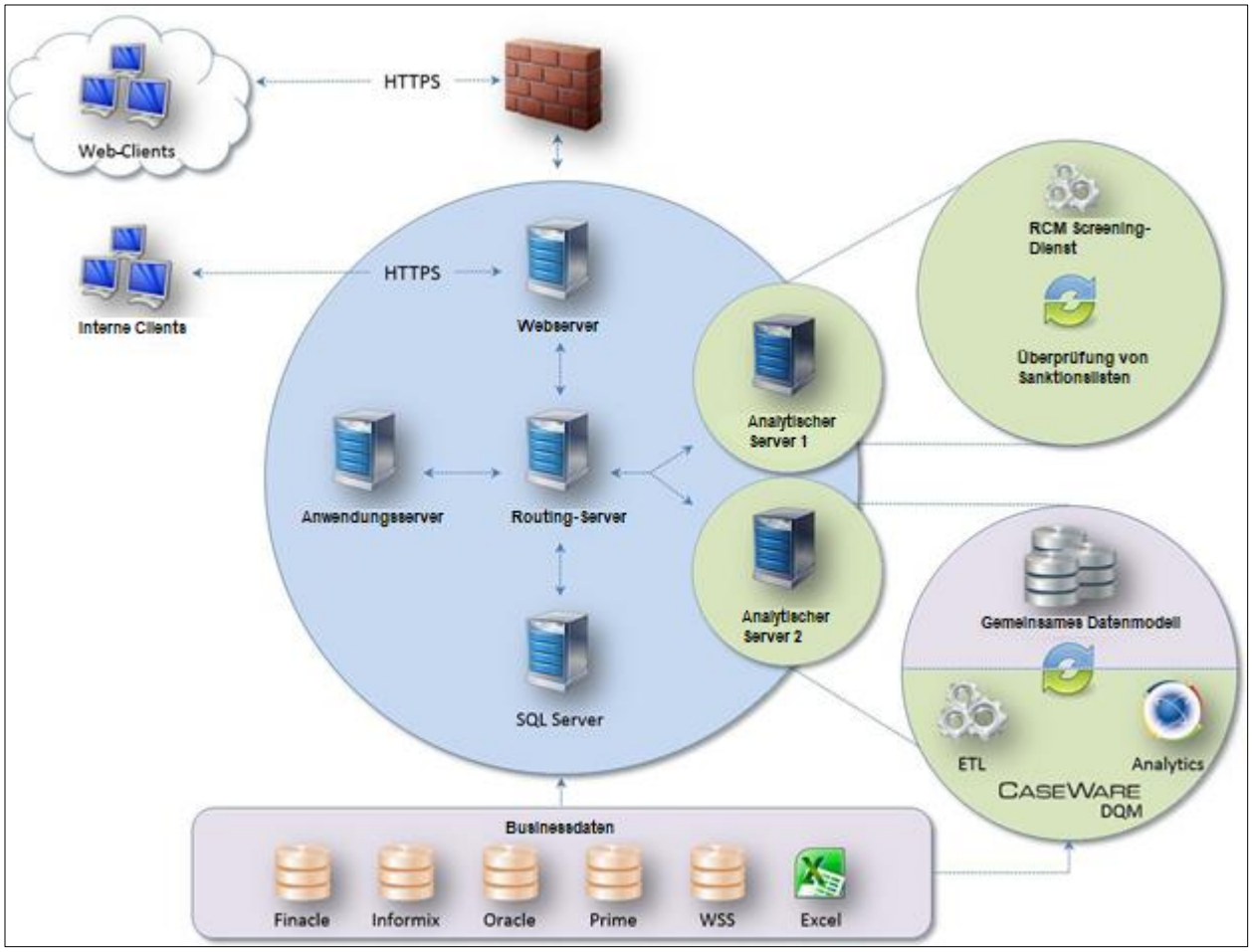
- Webanwendung
- Routing-Server
- Anwendungsserver
- Analytisches Modul-Server
- Instanzmanager

In der unten stehenden Abbildung ist die Alessa Architektur übersichtlich dargestellt. Die Hauptkomponenten des Systems wurden durch die Analyse einiger der bedeutendsten Anwendungsfälle im Continuous-Monitoring-Prozess identifiziert. Die Grafik zeigt die wichtigsten, für die Anwendungsfälle erforderlichen Systemkomponenten und stellt zusammengehörige Komponenten sowie Komponenten mit einer geringen Verbindung zueinander klar da, um eine höhere Wartungsfreundlichkeit und Agilität bei der Entwicklung zu ermöglichen.



Topologie

Aufgrund ihrer soliden Architektur ist die Anwendung in der Lage, auch komplexere Einsatzszenarien in einem Unternehmen zu meistern. Zur Verbesserung der Performance in verteilten Netzwerkumgebungen nutzt sie erweiterte Hardware-Ressourcen. Die Abbildung unten zeigt ein typisches Einsatzszenario der Anwendungskomponenten in einem Netzwerk.



Topologie der Anwendung

In der Abbildung oben sehen Sie, dass der Anwendungsserver, der Routing-Server sowie der Analytisches Modul-Server auf demselben oder auf unterschiedlichen Rechnern installiert sein können. Die Installation muss von einem Benutzer ausgeführt werden, der mit dem Netzwerk vertraut ist und über ausreichend Rechte in der Domäne verfügt, um jede Komponente auf der Servermaschine zu installieren.

Webanwendung

Die Webanwendung ist das Hauptportal der Anwendung. Dabei handelt es sich um eine ASP.NET 5.0-Anwendung, die auf Microsoft Information Systems (IIS) läuft. Außerdem werden die folgenden Technologien genutzt:

- Microsoft .NET Framework (4.8)
- EXT.JS
- EXT.NET
- JavaScript
- JGragh (Visualisierungsbibliothek)
- HTML 5
- CSS 3.0

Caching

Die folgenden Informationen sind in einem Cookie auf der Maschine des Benutzers gespeichert:

- Der Benutzername des Benutzers, der sich zuletzt erfolgreich angemeldet hat.
- Die Ländereinstellung (Locale) des Benutzers, der sich zuletzt erfolgreich angemeldet hat.

Sicherheit

Alessa unterstützt das HTTPS-Protokoll für die Kommunikation mit dem Webserver.

Routing-Server

Der Routing-Server ist ein ausführbares Programm, das als Windows-Dienst installiert ist. Er enthält mehrere selbstgehostete WCF-Dienste, die die für die Weiterleitung von Nachrichten an andere erforderliche Dienste notwendige Funktionalität umfassen. Der Routing-Server ist der Einstiegspunkt für diese Dienste und fungiert als zentrale Schnittstelle in dem Einsatzmodell von Alessa.

Die folgenden Technologien werden vom Routing-Server genutzt:

- Microsoft Message Queuing (MSMQ)
- Microsoft Distributed Transaction Coordinator (DTC)
- Microsoft .NET Framework (4.0)

Der Windows-Dienst ist der Host für die unten aufgeführten WCF-Dienste:

DIENST	PLUGIN-ASSEMBLY-PFAD	KOMMENTAR
Benachrichti-gung	RoutingServices\NotificationService	Verarbeitet Nachrichtenereignisse und bedient Schnittstellen zu unternehmensweiten Nachrichtensystemen (E-Mail-Server, SMS-Dienst, MSMQ).
Veröffent-lichung von Ereignissen an Abonnenten	RoutingServices\PublishingSubscriptionService	Verarbeitet Ereignisabonnements und veröffentlicht Ereignisse an Abonnenten, sobald sie auftreten. Bietet einen Hub für die Remote-Kommunikation zwischen Prozessen.
Routing	RoutingServices\RouterService	Leitet Benutzeranfragen an den entsprechenden Dienst weiter. Ermittelt neue Dienste im Netzwerk, wenn diese für die Weiterleitung zur Verfügung stehen. Ermöglicht einen Lastenausgleich durch die Weiterleitung von Benutzeranfragen.

Anwendungsserver

Der Anwendungsserver ist ein ausführbares Programm, das als Windows-Service installiert ist. Er umfasst mehrere selbstgehostete WCF-Dienste, die den Großteil der benutzerzentrierten Businesslogik der Lösung enthalten.

Die folgenden Technologien werden vom Anwendungsserver genutzt:

- Microsoft Message Queuing (MSMQ)
- Microsoft Distributed Transaction Coordinator (DTC)
- Microsoft .NET Framework 4.0

Der Windows-Dienst ist der Host für die unten aufgeführten WCF-Dienste:

DIENST	PLUGIN-ASSEMBLY-PFAD	KOMMENTAR
Prozessverwaltung	ApplicationServices\ BPManagementService	Verwaltungsdienst für Businessprozess-Funktionen. Dient primär der CRUD-Funktionalität (CRUD - Erstellen, Lesen, Aktualisieren und Löschen) für Prozesse, Aktivitäten, Kontrollen und Ergebnisgruppen.
Mitgliedschaft	ApplicationServices\ MembershipService	Verwaltungsdienst für die Authentifizierung und Autorisierung. Dient primär der CRUD-Funktionalität für Benutzer, Rollen und Mitgliedschaft.
Benachrichtigungs-subskription	ApplicationServices\ NotificationSubscriptionService	Verwaltungsdienst für Benachrichtigungsereignisse und Benutzerabonnements. Dient primär der CRUD-Funktionalität für Benachrichtigungen und Nachrichtenvorlagen.

Workflowmodul	ApplicationServices\ WorkflowEngineService	Ausführen von Workflowjobs, einschließlich automatischer Übertragungen, manueller Übertragungen und überfälliger Arbeitsaufgaben.
Workflow	ApplicationServices\ WorkflowService	Verwaltungsdienst für Workflows. Dient primär der CRUD-Funktionalität für Workflows, Teams und Vorlagen.

Analytisches Modul-Server

Der Analytisches Modul-Server ist ein ausführbares Programm, das als Windows-Dienst installiert ist. Er umfasst mehrere selbstgehostete WCF-Dienste, die die von der Lösung unterstützten analytischen Module enthalten.

Die folgenden Technologien werden vom Analytisches Modul-Server genutzt:

- Microsoft Message Queuing (MSMQ)
- Microsoft Distributed Transaction Coordinator (DTC)
- Microsoft .NET Framework 4.0

Der Windows-Dienst ist der Host für die unten aufgeführten WCF-Dienste:

DIENST	PLUGIN-ASSEMBLY-PFAD	KOMMENTAR
Datenanaly-tische Module	AnalyticEngineServices\ DataAnalysisEngineService	Verwaltungsdienst für analytische Module. Dient primär der Modulkonfiguration sowie der Vorgangsausführung. Alle Wrapper der analytischen Module werden von diesem Dienst gehostet.
Parameter	AnalyticEngineServices\ ParameterManagementService	Verwaltungsdienst für Parameter, die von den Scripting-Modulen verwendet werden. Dient primär der CRUD-Funktionalität (CRUD - Erstellen, Lesen, Aktualisieren und Löschen) für Parameter.
Skriptpaket	AnalyticEngineServices\ ScriptPackageService	Verwaltungsdienst für Skriptpakete. Dient primär der Funktionalität zur Dateiverwaltung und Versionierung für Pakete.
Vorgangs-verwaltung	AnalyticEngineServices\ TaskSchedulerService	Löst die Vorgänge aus, die für das Ausführen von Skripten aus Paketen terminiert sind. Dient primär der CRUD-Funktionalität für Vorgänge und dem Auslösen des analytischen Moduls zur Ausführung eines Paketskripts.

Instanzmanager

Über den Instanzmanager, der die Alessa Instanz auf dem aktiven Rechner anzeigt, können Sie die Windows-Dienste konfigurieren, die von Alessa installiert wurden, neue Anwendungsdienste bereitstellen und neue Datenmodule einsetzen.

Eine Alessa Instanz wird durch alle Komponenten, wie z. B. den Anwendungsserver, den Analytischen Modul-Server, den Routing-Server, die Web-Anwendung und die Lizenzen, definiert, die auf dem aktiven Rechner installiert sind.

Sicherheitsverwaltung und Zugriffsschutz

Das Sicherheitsmodell von Alessa besteht aus zwei Stufen. Stufe 1 bezieht sich auf die Nachrichtensicherheit und Stufe 2 auf den Zugriffsschutz der Anwendung.
Die Nachrichtensicherheit beschäftigt sich damit, wie Benutzer auf die Anwendung zugreifen und wie über das Netzwerk auf Dienste zugegriffen wird.
Auf dieser Stufe werden die Netzwerkzugangsdaten des Benutzers verwendet, um Dienstanforderungen zu authentifizieren. Der Benutzer muss ebenfalls auf Anwendungsebene authentifiziert werden, bevor er Zugriff über den Anmeldebildschirm der Anwendung erhält.

Der Zugriffsschutz der Anwendung definiert, wie Benutzer auf die unterschiedlichen Komponenten (Systemobjekte) und Funktionen der Anwendung zugreifen. Rechte können für die Konfigurationstools und jedes Objekt vergeben oder verweigert werden, das in der Anwendung erstellt wurde, einschließlich Berichte, Businessprozessobjekte, terminierte Vorgänge und erstellte Businessregeln.

Methoden der Benutzerauthentifizierung

Föderiertes Identitätsmanagement

Alessa verwendet Shibboleth Service Provider, um es in verschiedenen Identitätsverwaltungssystemen gespeicherten Benutzern zu ermöglichen, für den Zugriff auf Daten oder Dienste eine einzige digitale Identität zu nutzen. Shibboleth Service Provider ist eine Softwarelösung, mit deren Hilfe Webanwendungen wie Alessa Authentifizierungsanfragen verarbeiten können, die diese Identitäten verwenden. Sofern Ihr Unternehmen das föderierte Identitätsmanagement verwendet, können Sie Shibboleth Service Provider einsetzen, um sich mit dem Identity Provider Ihres Unternehmens bei Alessa anzumelden.

Datenbankauthentifizierung

Sie können Alessa neue Benutzer hinzufügen, indem Sie ein neues Benutzerkonto erstellen. Wenn Sie Benutzerkonten in Alessa erstellen, werden diese in der Alessa Datenbank gespeichert. Melden sich Benutzer bei Alessa an, werden deren Benutzernamen und Kennworte anhand der in der Alessa Datenbank hinterlegten Benutzernamen und Kennworte überprüft.

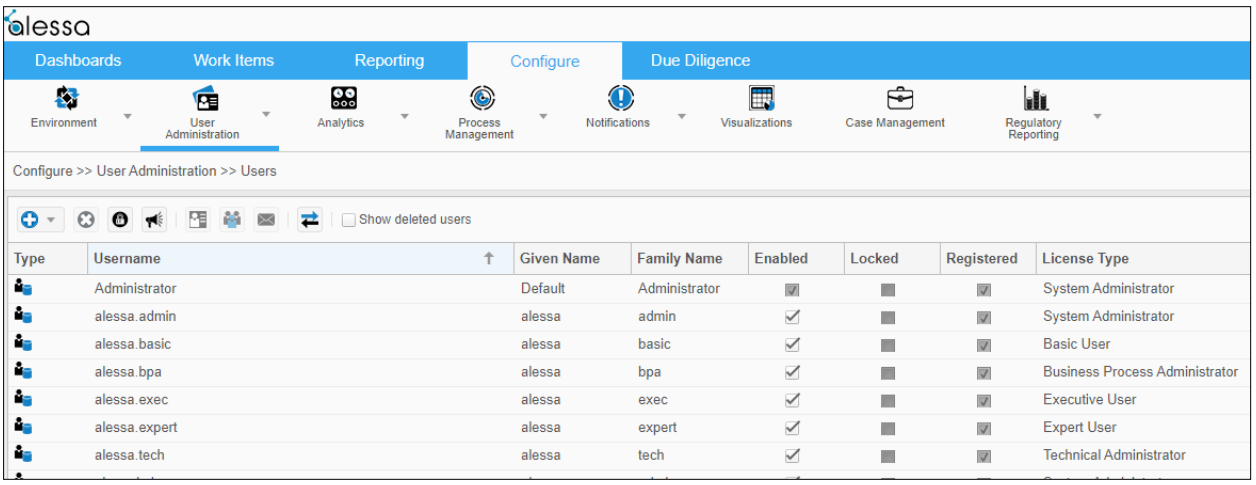
Windows-Authentifizierung

Sie können Benutzer aus dem Active Directory Ihres Unternehmens zu Alessa hinzufügen. Werden die Benutzer hinzugefügt, werden ihre Active Directory-Benutzernamen und Kontaktinformationen in die Alessa Datenbank kopiert. Die Benutzer können dann mit ihren Windows-Anmeldedaten auf Alessa zugreifen.

Benutzerverwaltung

Unternehmen können ihre Benutzer in Alessa auf der Seite **Benutzerverwaltung** verwalten (siehe Abbildung unten). Systemadministratoren können Funktionen wie das Erstellen, Löschen, Deaktivieren und Zuweisen von erforderlichen Berechtigungen an Benutzer ausführen. Außerdem sind Systemadministratoren in der Lage, Benutzerprofile zu aktualisieren und bei Bedarf Benutzerkonten zu entsperren.

Bitte beachten Sie, dass die Programmoberfläche erst nach Einspielen des Language-Packs in der jeweiligen sprachspezifischen Variante (z. B. auf Deutsch) angezeigt wird.



Benutzerverwaltung

Verwaltung des Benutzerkennworts

Das Alessa Kennwort muss wie folgt festgelegt sein:

- Es muss mindestens sechs Zeichen umfassen.
- Es darf maximal 128 Zeichen umfassen.

Kennwörter müssen mindestens ein Zeichen aus zumindest drei der folgenden Kategorien enthalten:

- Großbuchstaben
- Kleinbuchstaben
- Zahlen (0 -9)
- Nicht-alphanumerische Zeichen (z. B. @, #, $, *, &)

Kennwörter dürfen Folgendes nicht enthalten:

- Den Benutzernamen oder Teile davon oder drei oder mehr Zeichen des Namens in anderer Reihenfolge (z. B. Benutzername Janebrown und Kennwort nworbe1).

Die letzten fünf Kennworte werden nicht akzeptiert.

Datensicherheit

Die Konfiguration der Sicherheitsstufe für die Datenverschlüsselung obliegt allein dem Kunden und kann nach der Installation/Implementierung geändert werden. Alessa verwendet die WCF-Plattform (Windows Communication Foundation) für die gesamte Remote-Kommunikation zwischen den Softwarekomponenten. WCF ist eine auf SOAP-Nachrichten basierende verteilte Programmierplattform, die wiederum eine vielseitig einsetzbare und interoperable Plattform für den Austausch sicherer Nachrichten auf der Grundlage sowohl der bestehenden Sicherheitsinfrastruktur als auch der erkannten Sicherheitsstandards für SOAP-Nachrichten bietet. Die Sicherheit der Kommunikation kann gewährleistet werden, indem zwei Sicherheitsarten eingesetzt werden: Nachrichtensicherheit und Transportsicherheit.

Der Transportsicherheitsmodus verwendet ein Protokoll auf Transportebene, wie HTTPS, um die Übertragungssicherheit zu erreichen. Der Transportmodus hat den Vorteil, dass er weit verbreitet, auf vielen Plattformen verfügbar und weniger rechenaufwändig ist. Ein Nachteil besteht jedoch darin, dass Nachrichten nur von Punkt zu Punkt geschützt werden.

Der Nachrichtensicherheitsmodus nutzt hingegen die WS-Sicherheit (und weitere Spezifikationen), um die Übertragungssicherheit zu gewährleisten. Da die Nachrichtensicherheit direkt auf die SOAP-Nachrichten angewendet wird und zusammen mit den Anwendungsdaten innerhalb der SOAP-Pakete eingebunden ist, bietet dieser Modus den Vorteil, dass er unabhängig vom Transportprotokoll und erweiterbarer ist sowie - im Gegensatz zur Punkt-zu-Punkt-Sicherheit - eine Ende-zu-Ende-Sicherheit gewährleistet. Ein Nachteil besteht jedoch darin, dass der Nachrichtensicherheitsmodus wesentlich langsamer ist als der Transportsicherheitsmodus, da er mit dem XML-Charakter der SOAP-Nachrichten umgehen muss.

Durch den Einsatz bestehender Verschlüsselungsfunktionen in Microsoft SQL Server können Daten auch im Ruhemodus geschützt werden.

Datenintegration

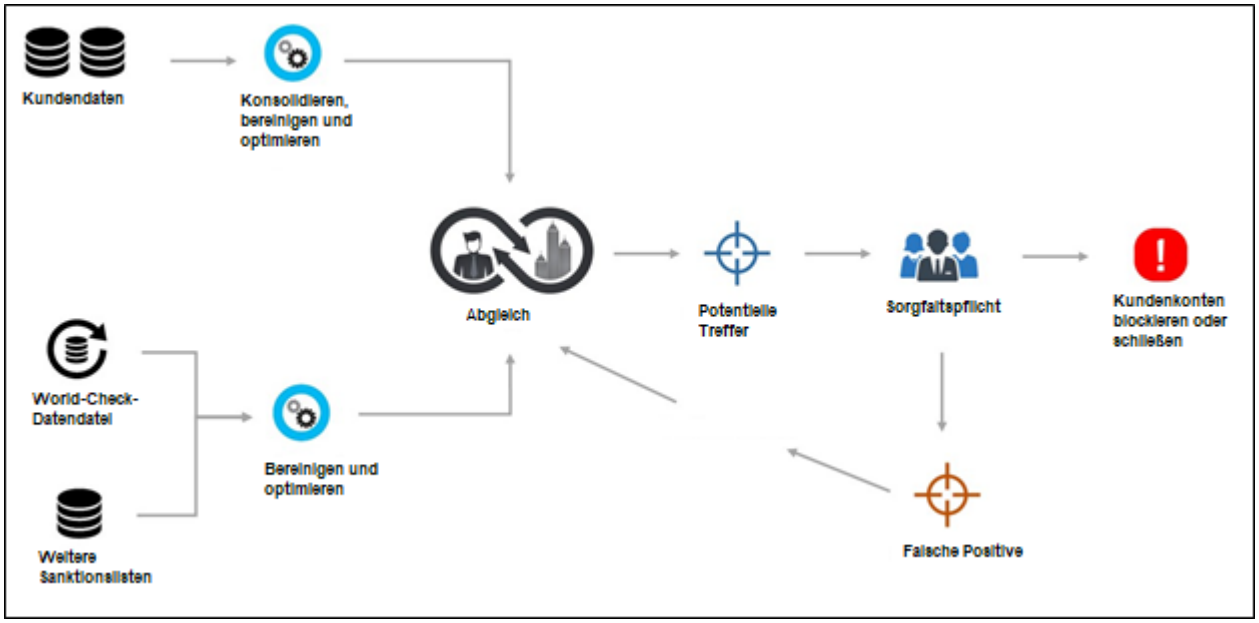
Alessa verwendet ETL-Tools, um Daten aus Quellsystemen zuzuordnen und zu extrahieren. Sobald die Daten extrahiert sind, werden diese von der Datenanalysesoftware verarbeitet und Ergebnisse generiert.

Alessa erfordert lediglich Lesezugriff auf die Unternehmensdaten und interagiert nicht direkt mit den Kernsystemen. Der Erstzugriff auf die Daten des Kernsystems erfolgt über die Datenimportfunktion des Scripting-Moduls, das entweder native Datenbanktreiber oder eine generische ODBC-Verbindung zu der zugrunde liegenden Datenbank einsetzt.

Die von Alessa unterstützen Scripting-Module können Daten aus jeder Datenquelle importieren. Diese Scripting-Module unterstützen die Verwendung nativer Treiber wie Microsoft Access und SAP/AIS sowie generische Treiber wie ODBC.

Datenfluss

Die Abbildung unten zeigt den Datenfluss bei der regelmäßigen Prüfung in Alessa. Sobald Warnungen generiert werden, werden diese in der Alessa Datenbank gespeichert, die auf einem Microsoft SQL Server gehostet wird.



Datenfluss

Strategie zur Notfallwiederherstellung

Die Architektur von Alessa besteht aus mehreren Schichten. Daher wird die Sicherung und Wiederherstellung für jede Schicht separat betrachtet.

Sicherung der Konfigurationsdaten in der Anwendungsschicht

Nach der Konfiguration von Alessa, die zu Beginn der Implementierung erfolgt, muss eine vollständige Sicherung der Businessprozesse stattfinden, die sich auf den Datenanalyse-Modul-Anwendungsservern befinden. Dies sollte stets wiederholt werden, sobald Änderungen an der Konfiguration der Businessprozesse vorgenommen werden.

In dem Fall, dass der verwendete Rechner nicht mehr einsatzfähig ist, kann Alessa auf einem anderen Rechner installiert werden und der Ordner **Businessprozess** kann durch die Backup-Datei ersetzt werden.

Empfohlen:

1. Legen Sie Images der Datenanalyse-Modul-Server an einem anderen Standort ab.
2. Behalten Sie eine Sicherungskopie der Businessprozessdateien, die nach der Durchführung von Konfigurationsänderungen erstellt wurde.

Im Falle von Datenverlust in dieser Schicht kann das Image wiederhergestellt werden und Kontrollen können innerhalb von Minuten ersetzt werden.

Sicherung der Datenbankschicht

Die zweite Stufe der Sicherung ist die Datenbanksicherung. Die verwendete Datenbank ist Microsoft SQL Server.

Empfohlen:
Das Notfallwiederherstellungsmodell von Alessa umfasst verschiedene Datenbankeinrichtungen. So werden Datenbankcluster synchron an zwei separate Orte gespiegelt sowie Sicherungskopien erstellt und an einem weiteren dritten Ort gespeichert. Alessa unterstützt native SQL-Funktionalität für die Notfallwiederherstellung, wie z. B. Sicherungen, Protokollversand, Replikation und SQL-Cluster etc.

(In diesem Fall beträgt die Uptime 99,99 % und der Datenverlust ist gleich Null. Für den Fall, dass ein Standort ausfällt, kann der Anwendungsserver innerhalb von Sekunden auf die gespiegelte Datenbank umgeleitet werden).

Anhang A: Matrix zur Software-Konformität

	Betriebssysteme			Browser		Daten-banken				Analytische Module			
	Windows Server 2016	Windows Server 2012 R2	Windows Server 2012	Firefox 68.x.x	Chrome 76.x.x.x	SQL Server 2017	SQL Server 2016	SQL Server 2012 R2	SQL Server 2012	CaseWare IDEA Client 10.1.x, 10.2.x, 10.3	CaseWare IDEA Client 9.1.x, 9.2	Arbutus 5.53	ACL 9.1, 9.3, 10, 11
Alessa Client 32 Bit				x	x								
Alessa Client 64 Bit				x	x								
Analytisches Modul-Server	x	x	x							x	x	x	x
Anwendungs-server	x	x	x										
Routing-Server	x	x	x										
Webserver	x	x	x										
Datenbankserver (beliebiges Windows-64-Bit-Serverbetriebs-system)						x	x	x	x				

Sie haben Fragen?
Kontaktieren Sie uns!

+49 211 520 59-430

sales@audicon.net

www.audicon.net

Besuchen Sie uns – gerne auch online – in einer unserer Niederlassungen in Düsseldorf oder Stuttgart.