



RECHT-TESTBED

Betriebskonzept

Projekttitel: Industrie 4.0 Recht-Testbed: Juristische Testumgebung und offenes Repository
Akronym: I4ORTB
Projektbeginn: 01.06.2019
Dauer: 48 Monate

Bezeichnung des Deliverable	Betriebskonzept
Aktuelles Datum	17.12.2021
Dokumentenversion	0.9
Autor	Timo Eler, Norbert Weiß

Gefördert durch:



aufgrund eines Beschlusses
des Deutschen Bundestages

Inhalt

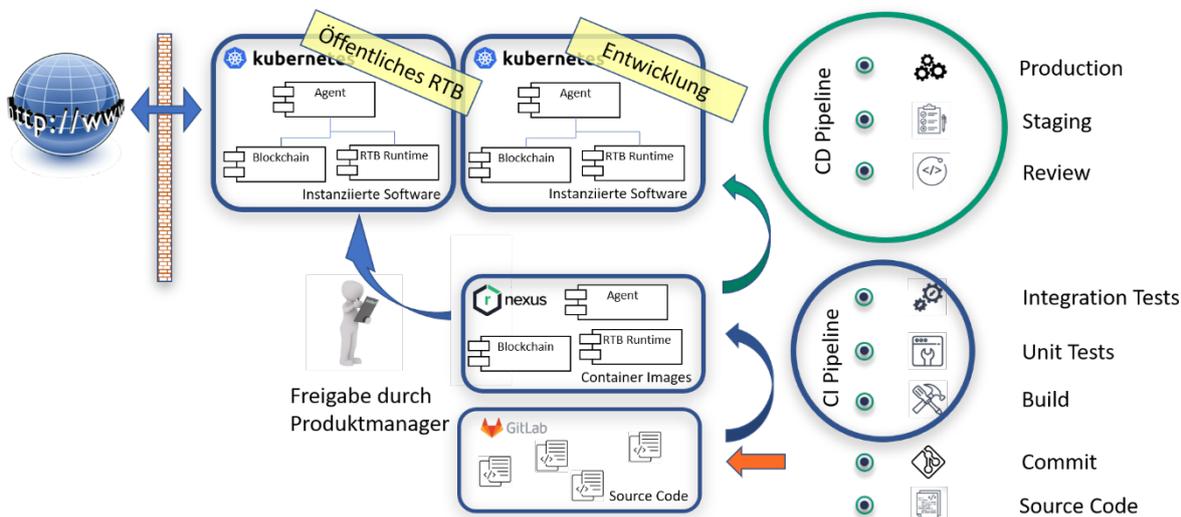
Kurzfassung	2
Systemübersicht	2
Rollen, Rechte und Pflichten	2
Systemadministrator RTB	2
Projektmanager	3
RTB-Entwickler	3
RTB Analyst.....	3
Prozesse.....	4
Einbringen neuer Artefakte in die öffentliche Infrastruktur	4
Erstellen von neuen Versionen und Bugfixes	4
Veröffentlichen von Source Code.....	4
Betrieb	4
Nutzerverwaltung und Authentifizierung	4
Verfügbarkeit.....	4
Backup	4
Sicherheit.....	4
Datenschutz.....	4
Wartung.....	5

Kurzfassung

Im Rahmen des Forschungsprojektes „Industrie 4.0 Recht-Testbed“ (RTB) wird ein öffentliches Experimentierfeld geschaffen, das es erlaubt, die automatische Aushandlung rechtsverbindlicher Verträge ohne menschliche Interaktion zu erproben. Dabei sollen sowohl juristische Fragestellungen wie auch Fragen der IT-Sicherheit beantwortet werden können. Mittels vordefinierter Szenarien können ausgewählte Use-Cases untersucht und in vielfältiger Parametrierung erprobt werden.

Das in diesem Dokument vorliegende Betriebskonzept beschreibt die entwickelte Infrastruktur sowie die technischen und organisatorischen Maßnahmen für deren Betrieb in einer Test- und einer Live Umgebung. Der Betrieb einer RTB Infrastruktur außerhalb der Live- oder Testumgebung ist möglich, aber nicht Teil des vorliegenden Betriebskonzeptes.

Systemübersicht



Rollen, Rechte und Pflichten

Systemadministrator RTB

Der Systemadministrator RTB ist für die Verfügbarkeit und Instandhaltung der Hard- und Software innerhalb der RTB-Infrastruktur verantwortlich. Es ist seine Pflicht, die RTB-Infrastruktur zu aktualisieren, gegen Angreifer zu sichern und nach außen hin verfügbar zu machen. Die RTB-Infrastruktur wird auf einem Kubernetes Cluster betrieben und nach außen durch eine Firewall geschützt. Die Bereitstellung des Kubernetes Clusters sowie der Firewall liegen nicht im Aufgabenbereich des Systemadministrators RTB.

Der System-Administrator teilt allen beteiligten Personen Störungen nach Bekanntwerden bzw. geplante Wartungszeiten mit. Weiterhin ist der System-Administrator für die Benutzerverwaltung und das Hinzufügen neuer Artefakte verantwortlich.

Es wird empfohlen, die Rolle des System-Administrators auf verschiedene Personen aufzuteilen, um einen sicheren Betrieb der RTB Infrastruktur zu gewährleisten.

In der Testumgebung unterstützt der Administrator die Entwickler beim Deployment von Artefakten und bei der Automatisierung von Deployment Prozessen.

Projektmanager

Der Projektmanager ist für die Fachlichkeit der öffentlichen Umgebung verantwortlich. Er entscheidet, welche Artefakte in die öffentliche RTB Infrastruktur deployed werden sollen.

Der Projektmanager ist dafür verantwortlich, dass die Lizenzen aller Artefakte gemäß den Vorgaben geprüft werden.

Die fortlaufende Dokumentation der Konfiguration ist Aufgabe des Projektmanagers. Sie umfasst eine Liste aller freigegebenen Artefakte.

Der Source Code der veröffentlichten Artefakte muss durch den Projektmanager vor der Veröffentlichung freigegeben werden.

RTB-Entwickler

Der RTB-Entwickler erstellt Quellcode für die Artefakte des RTB. Er ist verantwortlich für die Einhaltung der Lizenzbedingungen für abhängige Komponenten. Quellcode darf nicht aus dem Internet kopiert werden (z.B. aus GitHub Repository oder von StackOverFlow).

Der Entwickler ist verantwortlich für die Einhaltung der Code Richtlinien.

Der Quellcode ist mit Copy Right Hinweisen zu versehen und muss vor der Veröffentlichung die CI Pipeline durchlaufen und das Qualitygate bestehen.

Für jedes Projekt erstellt der Entwickler ein Readme.md mit einer Kurzbeschreibung des Projektes, Informationen zum Starten des Projektes und der Schnittstellen.

Abhängige Komponenten dürfen nur verwendet werden, wenn die Lizenz in der Liste der freigegebenen Lizenzen enthalten ist.

Der Entwickler stellt sicher, dass das Artefakt auch außerhalb von Fraunhofer aus dem Source Code mit öffentlich verfügbaren Werkzeugen erstellt werden kann.

Die Lizenz wird vom Entwickler jedem Projekt auf oberster Ebene beigefügt. Der Entwickler stellt eine automatisiert erstellte Liste aller verwendeten Lizenzen des Projektes für eine Lizenzprüfung durch den Projektmanager zur Verfügung.

RTB Analyst

Externe Benutzer, die auf die RTB Infrastruktur zugreifen, haben die Rolle RTB-Analyst

Der RTB-Analyst hat Zugriff über eine Weboberfläche auf das öffentliche Experimentierfeld.

Der RTB-Analyst kann mit den vom Projekt öffentlich bereitgestellten Szenarien experimentieren. Diese Szenarien repräsentieren die Usecases des Projektes mit fiktiven Unternehmen und Daten und dienen der Veranschaulichung.

Der RTB-Analyst kann im öffentlichen Experimentierfeld keine eigenen Daten und Komponenten einbringen, sondern nur die vorgegeben Daten beeinflussen, um mit den Szenarien zu experimentieren.

Es können mehrere RTB-Analysten gleichzeitig auf das Experimentierfeld zugreifen.

Es findet keine Authentifizierung statt.

Es werden keine spezifischen Daten auf dem Server gespeichert, die Ergebnisse der Experimente werden nur als Download zur Verfügung gestellt.

Prozesse

Einbringen neuer Artefakte in die öffentliche Infrastruktur

Alle Artefakte werden über Skripte, die einer Versionsverwaltung unterliegen, in das öffentliche Experimentierfeld eingebracht (deployed). Dabei werden die Artefakte in binärer Form aus einem nexus Repository entnommen.

Erstellen von neuen Versionen und Bugfixes

Neue Versionen dürfen nur in die Test Infrastruktur des RTB eingebracht werden. Binäre Artefakte werden immer von einer CI Pipeline erstellt und im nexus Repository abgelegt.

Veröffentlichen von Source Code

Es ist geplant, den Source Code des Experimentierfeldes, der beteiligten Artefakte, der Smart Legal Contracts und aller benötigter Skripte als Open Source zu veröffentlichen.

Betrieb

Nutzerverwaltung und Authentifizierung

Externe Nutzer werden nicht authentifiziert. Eine Nutzerverwaltung ist nicht Bestandteil des RTB Experimentierfeldes.

Verfügbarkeit

Für einen geregelten Betrieb eines RTB Experimentierfeldes muss die Verfügbarkeit definiert sein. Das Experimentierfeld ist verfügbar, wenn gilt:

- das Experimentierfeld ist über das Internet erreichbar
- die Eingabe von Daten zur Konfiguration von Szenarien ist möglich

Backup

Da das Experimentierfeld keine Daten aus den Experimenten speichert, muss hier kein gesondertes Backup erstellt werden. Das Backup des zugrunde liegenden Clusters wird durch das Fraunhofer IML bereitgestellt.

Wenn das Experimentierfeld wiederhergestellt werden muss, ist das aus der Versionsverwaltung jederzeit möglich.

Sicherheit

Die Kommunikation innerhalb des Kubernetes Clusters findet (un)verschlüsselt statt.

Die Kommunikation nach außen (https) findet SSL verschlüsselt statt. Die Zertifikate werden über die Fraunhofer Gesellschaft zur Verfügung gestellt und sind vom Administrator entsprechend zu installieren.

Das öffentliche Experimentierfeld wird in einer DMZ bereitgestellt. Zugriffe aus dem Internet sind nur auf freigegebene Ports (80 / 443) möglich. Aus dem Netz der Fraunhofer Gesellschaft sind unbeschränkte Zugriffe möglich, Zugriffe aus dem Netz des öffentlichen Experimentierfeldes in das Netz der Fraunhofer Gesellschaft sind nicht zulässig.

Datenschutz

Derzeit werden keine personenbezogenen Daten im Rahmen der fachlichen Prozesse erhoben oder verarbeitet. Die im Rahmen des IT-Betriebs anfallenden personenbeziehbaren Daten (z.B. Log Dateien) werden nach 30 Tagen automatisch gelöscht.

Wartung

Zeitfenster für die Wartung werden, wenn möglich, über die Webseite 5 Tage im Voraus angekündigt. Während der Wartung wird ein entsprechender Hinweis auf der Webseite veröffentlicht.