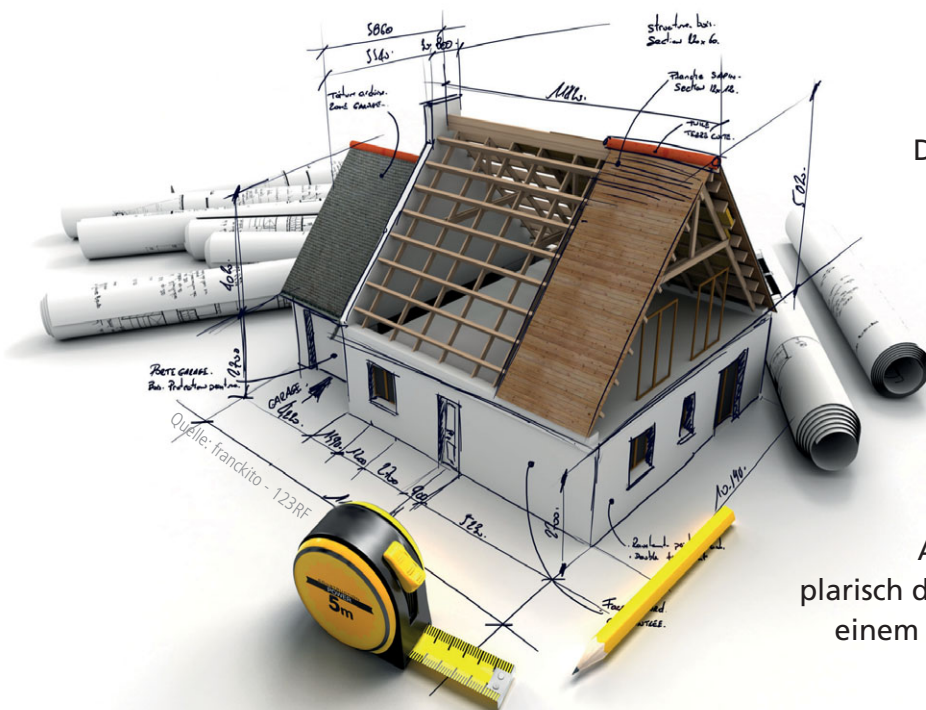


Planvoll umgesetzt

von Stefan Christoph,
Frank Blessing und Tufan Özdoğan

Das AWS Well-Architected Framework unterstützt IT-Verantwortliche bei der Entwicklung ausfallsicherer und effizienter Cloudinfrastrukturen für Unternehmensanwendungen. Wir zeigen in diesem Artikel auf, wie sich die Konzepte aus dem Framework in der Praxis umsetzen lassen. Dazu geben wir eine Einführung in das AWS Well-Architected Tool und schildern exemplarisch die ersten Schritte damit – gerade bei einem Well-Architected Framework Review gilt es einige Dinge zu beachten.



Um festzustellen, ob beim Cloud-design bewährte Methoden befolgt werden und gegebenenfalls Risiken im Aufbau oder dem Vorgehen bestehen, bietet sich ein Architekturreview an. Als Cloudanbieter hat AWS auf Basis von Daten Vorgehensweisen entwickelt, die sich in der Struktur und den Fragen des Well-Architected Framework Reviews widerspiegeln. Über die Jahre formalisierte der Anbieter entsprechende Prüfmechanismen – das Framework existiert bereits seit 2015. Anwendbar werden diese einheitlich zusammengestellten Best Practices für den Nutzer durch einen Fragenkatalog. Durch die Beantwortung lässt sich erkunden, wie gut eine Architektur mit den bewährten Methoden für die Cloud übereinstimmt. Darüber hinaus bietet das Framework detaillierte Anleitungen zur Verbesserung von gefundenen Schwachstellen.

Ziel des Well-Architected Framework ist es, ein gutes, dem Anwendungszweck gerechtes Design einer Applikation in der Cloud zu erreichen. Ein solches Prinzip ist zum Beispiel, Umgebungen datenge-

trieben zu entwickeln. Es geht darum, den Einfluss von Architekturentscheidungen zu messen und darauf basierend eine faktenbasierte Weiterentwicklung der Architektur zu betreiben. Dies ist mittlerweile durch das Sammeln von Metriken über den Änderungsprozess hinweg möglich. Jede neue Version der Architektur liefert neue Datenpunkte, auf deren Basis Unternehmen eine kontinuierliche Evolution planen können. Diese Datenpunkte lassen sich gezielt nutzen, um beispielsweise Verbesserungen umzusetzen.

Sechs Säulen als Grundlage

Das AWS Well-Architected Framework basiert auf sechs Säulen, die verschiedene Aspekte betrachten. Im Einzelnen sind dies die Punkte:

- Operative Exzellenz
- Sicherheit
- Zuverlässigkeit
- Leistung und Effizienz
- Kostenoptimierung und
- Nachhaltigkeit

Operative Exzellenz befasst sich mit der Ausführung und Überwachung der be-

reitgestellten Systeme. Ziele sind die Generierung eines tatsächlichen Mehrwerts für das Geschäft sowie die beständige Optimierung der Prozesse und Verfahren. Wichtige Aspekte dabei sind Automatisierung von Änderungen, der effiziente Umgang mit Störungen im Betrieb und die Definition von Standards für die Verwaltung des täglichen Betriebs. Darauf aufbauend geht es um die Themen effektive Organisation von Teams und Mittel zur Förderung von Innovation.

Die Säule Sicherheit betrifft den Schutz von Informationen und Systemen. Zu den wichtigsten Bereichen zählen hier Vertraulichkeit und Datenintegrität, Rechteverwaltung inklusive Festlegen und Verwalten individueller Berechtigungen, der Schutz von Systemen sowie die Einrichtung von Kontrollen zur Erkennung von Sicherheitsvorfällen.

Der Aspekt Zuverlässigkeit konzentriert sich darauf, sicherzustellen, dass der Workload seine vorgesehene Funktion zur richtigen Zeit korrekt und konsistent ausführt. Ein ausfallsicherer Workload

erholt sich im Idealfall schnell von Ausfällen, um den Unternehmensansprüchen gerecht zu werden. Wichtige Aspekte hierbei sind ein verteiltes Systemdesign, Wiederherstellungsplanung und die Handhabung von Veränderungen.

Der Pfeiler Leistung und Effizienz dreht sich um die effiziente Nutzung von IT- und Rechenressourcen. Zu den wichtigsten Themen zählen die Auswahl der richtigen Ressourcen auf Basis des Workloads, die Leistungsüberwachung sowie fundierte Entscheidungen zur Aufrechterhaltung der Effizienz auch bei wachsenden Geschäften.

Die Säule Kostenoptimierung hat die Vermeidung unnötiger Kosten zum Ziel. Der Schlüssel zum Erfolg dabei ist Sichtbarkeit auf die Kosten herzustellen, Budgets zu definieren und Ausgaben regelmäßig zu analysieren und darauf basierend kontinuierlich zu optimieren. Der Sektor Nachhaltigkeit schließlich befasst sich mit der Minimierung von Auswirkungen auf die Umwelt durch das Nutzen von Cloud-Workloads. Kernthemen sind das Modell geteilter Verantwortung für Nachhaltigkeit, Verständnis für die Auswirkungen auf die Umwelt und die optimale Ausnutzung vorhandener Ressourcen, um Auswirkungen auf die Umwelt zu reduzieren.

So läuft ein Review idealerweise ab

Der Grundstein für ein erfolgreiches Well-Architected Framework Review besteht unter anderem darin, von Anfang an einen konkreten, von allen gleich verstandenen Umfang des zu betrachtenden Workloads zu definieren. Das Explizit machen dieses Umfangs sorgt dafür, dass Sie zum einen die erforderlichen Wissensträger zu dem Review einbeziehen und zum anderen klare Abgrenzungen zu anderen Systemen ziehen können. Dies reduziert die Wahrscheinlichkeit von Verzögerungen während und nach dem Review erheblich, da sich die entscheidenden Informationen zum Workload im Meeting bereitstellen lassen und der Umfang der zu betrachtenden Bestandteile nicht kontinuierlich weiter wächst.

Wichtig ist weiterhin, dass Sie zusätzlich zu den technischen Kompetenzträgern

auch die Business-Seite mit zum Review-Meeting einladen. Nur so lassen sich alle den Workload ausmachenden Aspekte betrachten und im Nachgang Verbesserungen auf Basis der geführten Diskussionen definieren. Während es elementar ist, alle angesprochenen Bereiche des Well-Architected Framework Reviews mit den Teilnehmern abzudecken, ist es ebenso wichtig, die Teilnehmeranzahl zu begrenzen. In einer zu großen Gruppe ufern die wichtigen Diskussionen häufig zu sehr aus und es gestaltet sich schwer, das Review in einer angemessenen Zeit umzusetzen. Weniger ist hier häufig mehr.

Diskussionen im Review-Meeting sind gewollt und wertvoll. Häufig ist ein solches Treffen eine der wenigen Gelegenheiten, die alle relevanten Sichten vereint. Vermeiden Sie es aber, in unproduktive und detailverliebte Diskussionen abzugleiten. Hier ist eine aktive Moderation gefragt, die auf ein gemeinsames Ziel hinarbeitet. Diese Moderation ist gut bei erfahrenen Personen aufgehoben, typischerweise Cloudarchitekten, die nicht unmittelbar an dem Workload beteiligt sind und damit unvoreingenommen durch das Review führen können.

Notieren Sie Argumente und zusätzlich aufkommende Themen und greifen sie sie zu einem späteren Zeitpunkt auf. Sollte es nicht möglich sein, sich auf eine gemeinsame Beantwortung einer Frage zu einigen, halten Sie auch das fest. Sehr oft kommt es vor, dass durch solche Diskussionen während des Reviews Informationslücken sichtbar werden, die sich im Anschluss schließen lassen.

Beziehen Sie Bedenken des Teams ein

Es ist wichtig, vor dem eigentlichen Review zu definieren, zu welchem Zweck dieses Review erfolgt. Motivationen können mannigfaltig sein. Es könnte beispielsweise sein, dass das für den Workload verantwortliche Team für sich selber analysieren möchte, welche Schwachstellen die aktuelle Architektur des Workloads hat. Mängel können dabei häufig schnell analysiert werden. Aber auch in diesem Fall ist sicherzustellen, dass keine beteiligte Person Scheu davor hat, Fehler einzugestehen,

oder versucht ist, die eigene Arbeit zu verteidigen oder in einem besseren Licht dastehen zu lassen. Dies erreichen Sie am einfachsten, wenn Sie vorab klären, dass die Ergebnisse des Reviews nur im Kreis der unmittelbar Beteiligten verbleiben.

Eine andere Motivation könnte sein, gefundene Schwächen und die aus der Behebung anstehenden Aufwände zu dokumentieren, um darauf basierend zusätzliche Ressourcen, wie Mitarbeiter oder Zeit, einzufordern. Wird dieses klar kommuniziert, sollten Sie ebenfalls zu guten Ergebnissen kommen.

Am schwierigsten ist es, wenn ein Review von außen angesetzt ist, beispielsweise durch das Management, oder gar mit der Motivation verbunden ist, Datenpunkte für ein externes Audit zu liefern. Hier müssen Sie viel Aufwand darauf verwenden, trotz dieser potenziell unangenehmen Situation eine vertrauensvolle Umgebung zu schaffen, in der Probleme offen angesprochen werden können. Der Moderator eines solchen Reviews muss Antworten umso kritischer hinterfragen, um das Ziel eines realistischen Review-Ergebnisses zu erreichen.

Ein wichtiger Aspekt ist es, die Mentalität der Teilnehmer zu justieren. Eine festgestellte Unzugänglichkeit – auch wenn sie mit einem hohen Risiko verbunden ist (High-Risk-Item) – dokumentiert kein Versagen, sondern die Möglichkeit, eine Verbesserung vorzunehmen. Dabei ist es gut, dies bereits in einem Review festzustellen und nicht erst dann, wenn das Risiko eintritt und gegebenenfalls einen Produktionsausfall provoziert.

Framework an eigene Workloads anpassen

Das Ziel des Well-Architected Frameworks ist es, einheitliche Prinzipien und bewährte Methoden zur Verfügung zu stellen, die sich auf viele verschiedene Workloads anwenden lassen. Der generalistische Ansatz zielt hierbei auf ein möglichst breites Spektrum an Fragen ab. Nicht alle müssen auf den zu untersuchenden Workload zutreffen und können deshalb, gegebenenfalls für den Moment, ausgeblendet und mit einem entsprechenden Kommentar ver-

The screenshot displays the AWS Well-Architected Tool interface. On the left, a navigation pane shows the 'Security' section with 10 questions, 3 of which are completed. The main area is titled 'AWS Well-Architected Framework' and shows 'SEC 4. How do you detect and investigate security events?'. Below this, there are checkboxes for various logging and monitoring options, and a 'Notes - optional' section. On the right, a 'Helpful resources' sidebar lists links to AWS documentation and a 'Configure service and application logging' section.

1 Security 3/10

Well-Architected Tool > Workloads > Retail Website > AWS Well-Architected Framework > Review workload

2 AWS Well-Architected Framework

Add a link to your architectural design

3 Helpful resources

Ask an expert

SEC 4. How do you detect and investigate security events? Info

Ask an expert

Capture and analyze events from logs and metrics to gain visibility. Take action on security events and potential threats to help secure your workload.

☐ Question does not apply to this workload Info

Select from the following

☐ Configure service and application logging Info

☐ Analyze logs, findings, and metrics centrally Info

☐ Automate response to events Info

☐ Implement actionable security events Info

☐ None of these Info

► Mark best practice(s) that don't apply to this workload

Notes - optional

2084 characters remaining

Save and exit Previous Next

Helpful resources

Threat management in the cloud: Amazon GuardDuty and AWS Security Hub

Remediating Amazon GuardDuty and AWS Security Hub Findings

Centrally Monitoring Resource Configuration and Compliance

Setting up Amazon GuardDuty

AWS Security Hub

Amazon CloudWatch

Getting started: Amazon CloudWatch Logs

Amazon EventBridge

AWS Config

AWS Answers: Centralized Logging

Security Partner Solutions: Logging and Monitoring

Configure service and application logging

Configure logging throughout the workload, including application logs, resource logs, and AWS service logs. For example, ensure that AWS CloudTrail, Amazon CloudWatch Logs, Amazon GuardDuty and AWS Security Hub are enabled for all accounts within your organization.

Analyze logs, findings, and metrics centrally

All logs, metrics, and telemetry should be collected centrally, and automatically analyzed to detect anomalies and indicators of unauthorized activity. A dashboard can provide you easy to access insight into real-time health. For example, ensure that Amazon GuardDuty and Security Hub logs are sent to a central location for alerting and analysis.

Automate response to events

Using automation to investigate and remediate events reduces human effort and error, and enables you to scale investigation capabilities. Regular reviews will help you tune automation tools, and continuously iterate. For example, automate responses to Amazon GuardDuty events by

Die Fragenseite des AWS Well-Architected Tool ist in die drei Bereiche Navigation, Frage und Hintergrundwissen unterteilt.

sehen werden. Dies erlaubt es, den Fragenkatalog auf den für den Workload zutreffenden Umfang anzupassen.

Die Ergebnisse eines Reviews können vielfältig sein und unterschiedlich genutzt werden. In den allerseltensten Fällen dürfte das Resultat lauten: Alles ist perfekt umgesetzt und es gibt keine weiteren Empfehlungen. Aber selbst dann ist ein solches Review extrem wertvoll, da Sie nun die Gewissheit haben, dass der Anwendungsfall grundsätzlich gut aufgesetzt ist. Beim Großteil der Reviews ergibt sich jedoch eine Anzahl von festgestellten Risiken zusammen mit konkreten Lösungsvorschlägen und Empfehlungen. Dies ist ein idealer Startpunkt, um diese Aufgaben in die Planung für die nächsten Releases aufzunehmen und eine Priorisierung basierend der identifizierten Risiken vorzunehmen.

In die Welt der agilen Methoden übersetzt, ist das Ergebnis eines Well-Architected

Framework Reviews eine Anzahl von User Stories, die bereits gut qualifiziert sind, um zur Priorisierung in das Backlog überführt werden zu können. Bildlich gesprochen verlässt das Team nach dem Review einen Tisch voll mit Post-its.

Zukunftsgerichtet ergibt es Sinn, das Review in regelmäßigen Abständen (beispielsweise bei kontinuierlicher Weiterentwicklung des Workloads) oder bei größeren Änderungen erneut durchzuführen, um ein aktuelles Bild zu behalten.

Nutzung des Well-Architected Tool

Die Umsetzung des Frameworks führen Sie direkt in der AWS Management Console mit dem AWS Well-Architected Tool durch. Melden Sie sich in der Konsole an und öffnen Sie unter [1] das Werkzeug. Wenn Sie das Tool zum ersten Mal verwenden, erhalten Sie eine Seite mit einer Einführung in seine Funktionen angezeigt.

An erster Stelle müssen Sie einen Workload definieren. Wählen Sie dazu im Abschnitt "Define a workload" die Option "Define workload" aus. Alternativ können Sie im linken Navigationsbereich die Option "Workloads" und anschließend "Define workload" anklicken.

Für Einzelheiten darüber, wie AWS die Daten zu Ihrem Workload verwendet, wählen Sie "Why does AWS need this data, and how will it be used?" aus. Geben Sie im Feld "Name" einen Namen für Ihren Workload ein. Dieser muss zwischen drei und 100 Zeichen lang sein. Mindestens drei Zeichen dürfen keine Leerzeichen sein. Namen von Workloads müssen einzigartig sein. Leerzeichen und Groß-/Kleinschreibung werden aber ignoriert, wenn das System auf Einzigartigkeit prüft.

Geben Sie nun im Feld "Description" eine Beschreibung des Workloads ein. Diese muss zwischen drei und 250 Zeichen lang

sein. Tippen Sie im Anschluss im Feld "Review owner" den Namen, die E-Mail-Adresse oder den Identifizierungsschlüssel für die primäre Gruppe oder die primäre Person ein, die Eigentümer des Workload-Überprüfungsprozesses ist. Wählen Sie dann im Feld "Environment" die Umgebung für Ihren Workload aus: Ein Production-Workload läuft in einer Produktionsumgebung, ein Pre-Production-Workload läuft in einer Pre-Produktionsumgebung. Wählen Sie im Abschnitt "Regions" die Regionen für Ihren Workload aus. Hier können Sie sich zwischen AWS-Regionen und Nicht-AWS-Regionen entscheiden, bis zu fünf Regionen (getrennt durch Kommas) sind erlaubt. Es ist kein Problem, beide Optionen zu verwenden, falls dies auf Ihren Workload zutrifft.

Die folgenden Schritte sind optional: In der "Account-IDs"-Box können Sie die Account-IDs, die mit Ihrem Workload zusammenhängen, angeben. Im Feld "Architectural design" ist es möglich, die URL für Ihren Architekturentwurf einzutippen. Im Feld "Industry type" hinterlegen Sie die Art der Branche im Zusammenhang mit Ihrem Workload und im Feld "Industry" die genaue Branche selbst, die Ihrem Workload am besten entspricht. In der "Tag"-Sektion können Sie ferner Tags angeben, die ihrem Workload zugeordnet sein sollen. Klicken Sie danach auf "Weiter" – wenn ein erforderliches Feld leer oder ein angegebener Wert nicht gültig ist, müssen Sie das Problem zuerst beheben, bevor Sie fortfahren.

Wählen Sie nun noch die Perspektiven aus, die für diesen Workload gelten. Bis zu 20 davon lassen sich zu einem Workload hinzufügen – im Zuge dieses Artikels fokussieren wir uns jedoch auf die AWS-Well-Architected-Framework-Perspektive. Sie stellt grundlegende Fragen zu Ihrem Workload. Klicken Sie nun abschließend auf "Define workload". Nach dieser Definition bekommen Sie eine Seite mit den aktuellen Details Ihres Workloads angezeigt. Wählen Sie "Start reviewing" aus, um zu beginnen. Andernfalls können Sie im linken Navigationsbereich auf die Option "Workloads" sowie den Namen des Workloads klicken, um seine Detailseite zu öffnen.

Review-Fragen passend beantworten

Die Fragenseite des Reviews ist in drei Bereiche unterteilt: Im linken erscheinen die Fragen für jede der eingangs erwähnten Säulen. Fragen, die Sie beantwortet haben, sind mit "Done/Fertig" markiert. Die Anzahl der Fragen, die in jeder Säule beantwortet wurden, stehen neben deren Namen. Sie können zu Fragen in anderen Säulen navigieren, indem Sie den Namen der Säule und anschließend die Frage auswählen, die Sie beantworten möchten.

Im mittleren Bereich sehen Sie die aktuelle Frage. Wählen Sie die bewährten Methoden aus, die Sie befolgen. Klicken Sie auf "Info", um zusätzliche Informationen zur Frage oder einer bewährten Methode zu erhalten. Klicken Sie auf "Fragen Sie einen Experten", um auf den dedizierten AWS-Well-Architected-Bereich der AWS-Community re:Post zuzugreifen. Im rechten Bereich erscheinen zusätzliche Informationen und hilfreiche Ressourcen.

Gehen Sie beim Beantworten jeder Frage wie folgt vor: Lesen Sie die Frage und entscheiden Sie, ob sie auf Ihren Workload zutrifft – weitere Anleitungen finden Sie unter "Info". Trifft eine Frage nicht auf Ihren Workload zu, wählen Sie "Question does not apply to this workload". Andernfalls klicken Sie in der Liste auf die bewährten Methoden, die Sie derzeit befolgen. Wenn Sie derzeit keine dieser bewährten Ansätze nutzen, entscheiden Sie sich für "None of these".

Wenn eine oder mehrere bewährte Methoden nicht auf Ihren Workload zutreffen, markieren Sie bei "Best Practice" die Methoden ab, die nicht für diesen Workload gelten. Für jede abgewählte Best Practice können Sie optional einen Grund festlegen und zusätzliche Details angeben. Generell lässt sich optional auch das Feld "Notes" verwenden, um Informationen im Zusammenhang mit der Frage hinzuzufügen. Beschreiben Sie hier beispielsweise, warum die Frage nicht zutrifft oder stellen Sie zusätzliche Details zu den ausgewählten bewährten Methoden bereit.

Wählen Sie nach jeder Frage "Next" aus, um mit der nächsten fortzufahren. Sie können


jederzeit auf "Save and exit" klicken, um Ihre Änderungen zu speichern und die Dokumentation Ihres Workloads zu unterbrechen. Um zu den Fragen zurückzukehren, gehen Sie zur Detailseite des Workloads und klicken Sie auf "Continue review".

Nachdem Sie den Status Ihres Workloads zum ersten Mal dokumentiert haben, sollten Sie einen Meilenstein speichern und einen Workload-Bericht erstellen. Ein Meilenstein erfasst den aktuellen Status des Workloads und ermöglicht es Ihnen, künftigen Fortschritt zu messen, wenn Sie Änderungen basierend auf Ihrem Verbesserungsplan vornehmen.

Klicken Sie dazu auf der Detailseite des Workloads bei der Workload-Übersicht auf die Schaltfläche "Meilenstein speichern" und tippen Sie beispielsweise "Version 1.0 - Initial Review <Workload-Name>" ein. Vergessen Sie nicht, noch auf "Save" zu klicken.

Um hingegen einen Workload-Bericht zu generieren, wählen Sie die gewünschte Perspektive aus und klicken Sie auf "Generate report". Es wird eine PDF-Datei erstellt, die den Status des Workloads, die Anzahl der erkannten Risiken und eine Liste der empfohlenen Verbesserungen enthält.

Fazit

Das Review kann aufgrund des Umfangs der Fragen und der organisatorischen Hürden im Zuge eines interdisziplinären Austauschs eine Herausforderung darstellen. AWS-Teams oder -Partner unterstützen bei der Durchführung und können als unabhängige Partei das Review moderieren und schon währenddessen Fragen beantworten. Im Anschluss lassen sich dann gezielt Verbesserungen planen. Für die bessere Nachvollziehbarkeit können Teams die Verbesserungspotenziale als Tasks in ein Tool zum Ticketmanagement überführen. Auch ist es sinnvoll, den Workload kontinuierlich gegen die bewährten Methoden aus dem Well-Architected Framework Review zu messen. (In) 

Link-Codes

[1] AWS Well-Architected Tool
n2p21