

The Cloud Chapters – Special

19.01.2022 | SPIE Focus Series

SPIE ICS & Corporate Software

SPIE, sharing a vision for the future

Ausgangslage und Herausforderungen

19.01.2022 | Patrick Sommer

SPIE ICS & Corporate Software

SPIE, sharing a vision for the future

Case Study System IDAG



Primo Amrein • 1.

Cloud Lead at Microsoft / Startup Board Member

1 Monat • 🌐

(English follows) Das Bundesamt für Rüstung armasuisse setzt Azure und die Power Platform ein im Kampf gegen Covid. «Ohne die Sicherheit der Schweizer Microsoft Cloud und einer 20-jährigen Zusammenarbeit zwischen Bund und Microsoft hätte armasuisse und der KSD nicht auf diese Infrastruktur setzen können.»

Ein BI-Dashboard in Rekordzeit

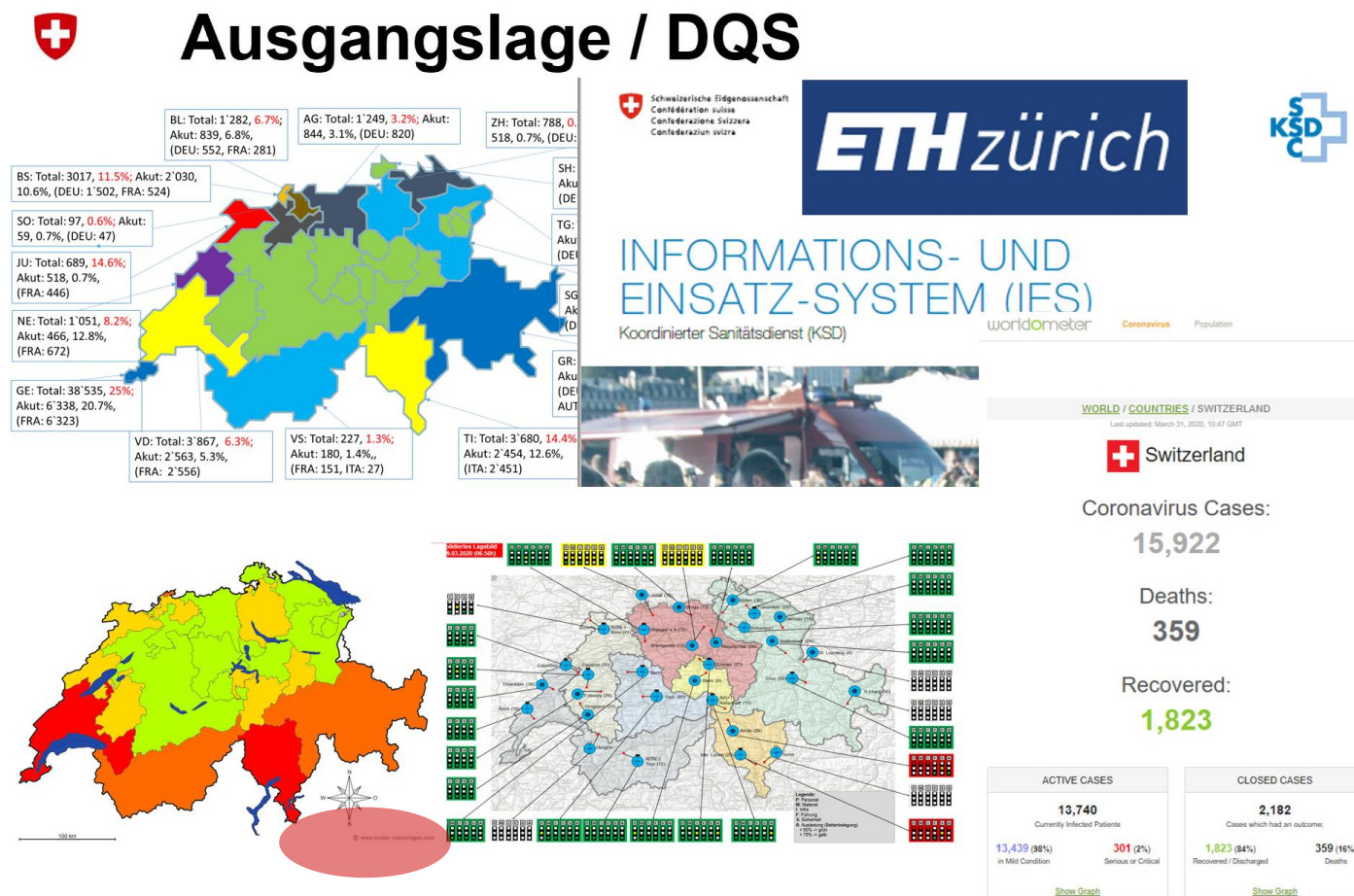
Im September 2020 folgte der Startschuss zum dringlichen Projekt, das die unterschiedlichen Datenströme automatisch aggregiert und für schnelle Auswertungen verfügbar macht. **In nur 45 Tagen** – so der ambitionierte Plan – **sollte geschafft werden, was auf regulärem Weg ein bis zehn Jahre dauern kann.** Jean-Paul Costa, Projektleiter bei armasuisse, gesteht: **“Alle – sogar ich selbst – haben gesagt: Das ist unmöglich!** Ich bin stolz auf das ganze Team – KSD, Microsoft, armasuisse und ganz besonders Corporate Software als Lösungs- und Implementationspartner, dass wir das neue Dashboard in der geforderten Qualität in dieser Rekordzeit zur Verfügung gestellt haben.

Ausgangspunkt

- **Koordinierten Sanitätsdienstes (KSD):** stufengerechte Koordination des Einsatzes und der Nutzung der personellen, materiellen und einrichtungsmässigen Mittel der zivilen und militärischen Stellen, die mit der Planung, Vorbereitung und Durchführung von sanitätsdienstlichen Massnahmen beauftragt sind.
- Der Koordinierte Sanitätsdienst (KSD) erhebt mit dem Informations- und Einsatzsystem IES regelmässig in **150 Akutspitälern** die Zahlen zu den **Spitalkapazitäten**. Sie dienen der Lagebeurteilung auf Stufe Bund und erlauben einen regionalen bis nationalen Ausgleich der Auslastung der Spitäler.



Ausgangspunkt



- Unterschiedliche isolierte Systeme
- Unterschiedliche Daten



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

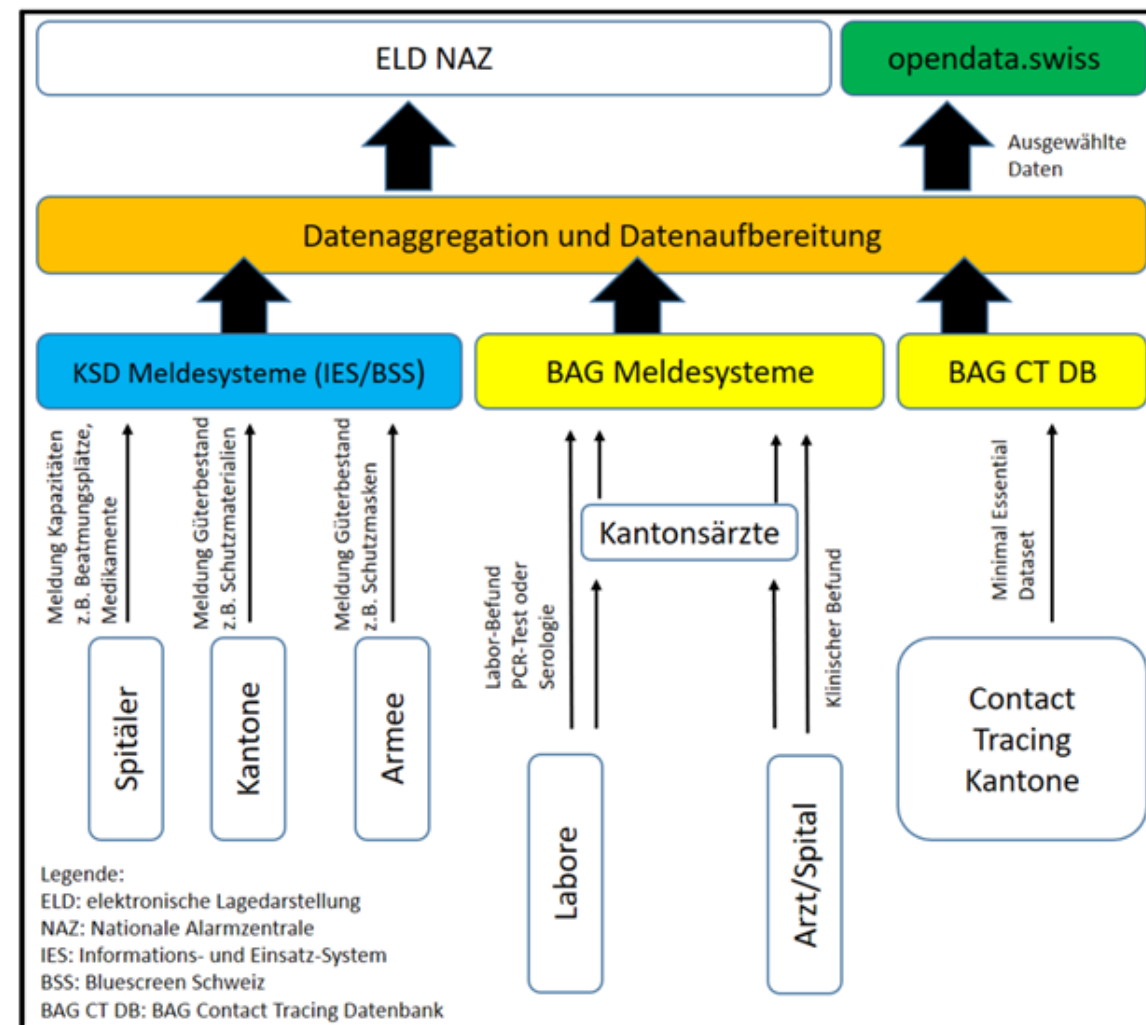
Bundesamt für Rüstung armasuisse

● COVID-19 Verordnung 3:

- › **Bundesratsbeschluss Mitte September 2020** und der aktualisierten COVID-19 Verordnung 3
- › Interdepartementale Arbeitsgruppe medizinische Güter (**IDAG**) welche diversen unterstützenden Aufgaben, namentlich im Kontext der Beschaffung und Zuteilung wichtiger medizinischer Güter übernimmt.
- › Zur Ausführung der Aufgaben soll ein „**System IDAG**“ zur Verfügung gestellt werden
 - ▶ Lagebeurteilung relevanten Informationen (Daten)
 - ▶ Daten der verschiedenen Meldesysteme möglichst automatisiert zusammenträgt
 - ▶ Daten aus weiteren Quellen anreichert
 - ▶ Informationen der IDAG bzw. den involvierten Bundesstellen zur Verfügung stellt
 - ▶ Berichte und Dashboards anhand der Vorgaben der involvierten und verantwortlichen Bundesstellen erstellen

Herausforderungen

- Komplexität
- Datenqualität
- Aktualität der Daten (Refresh)
- Regulationen / bundesinterne Abläufe



Herausforderungen

Pressekonferenz „Point de Presse Coronavirus“, Dienstag 27. Oktober 2020



- **Kritikalität**
- **Zeitdruck**
 - › Heute Bedarf aus Business
 - › Morgen implementiert
 - › Übermorgen erweitert
- **Zeitdruck System IDAG**
 - › 17.09.: Verordnung
 - › 24.09.: erstes Meeting
 - › 25.09.: Anforderungen
 - › 05.10.: Bestellung
 - › 27.10.: goLive
 - › 15.11.: Release 1.1
 - › ...

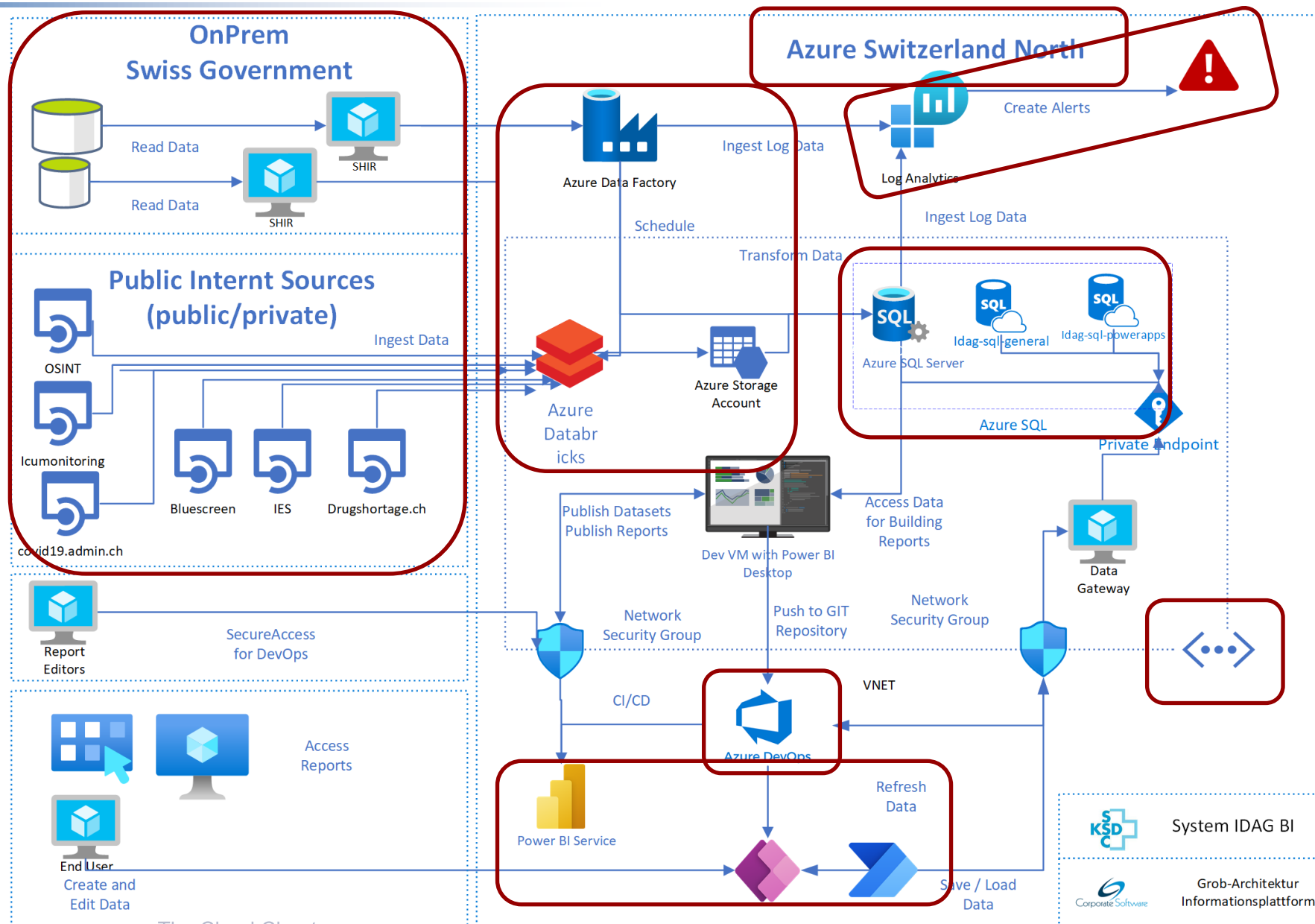
- Roman Kahr, Cloud Solution Architekt, Microsoft

IDAG Architektur

19.01.2022 | Roman Kahr

Microsoft

SPIE, sharing a vision for the future



Mehrwert aus Sicht Kunde

- Mit den eintreffenden Daten koordiniert der KSD die verfügbaren Ressourcen wie Material, freie Spitalbetten, Fachpersonen und Militärdienstleistende.
- **Jedoch wurden die Daten bis September 2020 manuell aufbereitet**
- Neu: Automatisierung der Datenströme
- Mario Kaufmann, KSD:
 - › Jetzt kann ich per Knopfdruck und immer aktuell auf die brennendsten Fragen Auskunft geben.”

Mehrwert aus Sicht Kunde

- Zusammenhänge zwischen Fallzahlen und Spitalbelegung können nun besser und schneller dargestellt werden.
- **Eine geographische Darstellung des Pandemieverlaufs und somit der regionalen Belastung war vor der Implementierung des Dashboards kaum möglich.**

Mehrwert aus Sicht Kunde

- Demokratisierung der Daten
- Datenbasis und die daraus gezogenen Erkenntnisse einfach und schnell für die involvierten Stellen wie Bund und die Armeeapotheke zur Verfügung zu stellen.
- Mario Kaufmann, KSD:
 - › “Ich bekam viele “Mercis” von den Benutzern dafür, dass sie nun selber Zugriff auf akkurate Daten haben und schneller reagieren können”

Mehrwert aus Sicht Kunde

- Was auch nach der Pandemie bleibt:
 - › Die neu gewonnene Erfahrung im **Umgang mit Agilität und der Cloud** für die Bewältigung von Krisensituationen.
 - › Dieser für den Bund unübliche Ansatz kann gemäss Jean-Paul Costa, armasuisse in Zukunft in kleinen Projekten weiter verfeinert und exploriert werden:
 - ▶ “Das nächste Virus kommt leider bestimmt.
 - ▶ Dieses Projekt hat uns gezeigt, wie wir schnell und agil auf Krisen reagieren können.
 - ▶ Wir haben enorm viel über uns selbst gelernt und wissen nun, wie wir unsere Daten für die Verteidigung auch gegen unsichtbare Feinde noch besser nutzen können.”

Theorie und Praxis

19.01.2022 | Raphael Fäh & Matthias Rückemann

SPIE ICS & Corporate Software

SPIE, sharing a vision for the future

Theorie und Praxis – Eine Übersicht

Cloud Chapter 2021 Inhalte ...

<p>05.03.2021</p> <p>Swiss Public Cloud Bund beschafft sich Public Cloud Services</p> <p>Patrick Sommer</p> <p>New & Innovative</p>	<p>05.03.2021</p> <p>Warum Kunden von ISO 27K zertifizierten CSPs profitieren können?</p> <p>David Mantock</p> <p>Security</p>	<p>05.03.2021</p> <p>Warum Sie das Cloud Adoption Framework unbedingt kennen müssen!</p> <p>Matthias Gessenay</p> <p>Governance</p>	<p>05.03.2021</p> <p>Business Continuity Management in der Cloud Eine Übersicht</p> <p>Matthias Rückemann</p> <p>Business Continuity</p>
<p>06.05.2021</p> <p>HyperScale Cloud Computing "Industrialization of IT"</p> <p>Patrick Sommer</p> <p>New & Innovative</p>	<p>06.05.2021</p> <p>Secure Cloud Transformation Sicherheit als Business Enabler!</p> <p>David Mantock</p> <p>Security</p>	<p>06.05.2021</p> <p>Am Ende kommt die Abrechnung: Wie Sie Cloud-Kosten unter Kontrolle behalten.</p> <p>Matthias Gessenay</p> <p>Governance</p>	<p>06.05.2021</p> <p>Design von Cloud Backup Services. Ich sichere meine Daten. Aber wie und wohin?</p> <p>Matthias Rückemann</p> <p>Business Continuity</p>
<p>10.06.2021</p> <p>Moderne Informationsplattformen Agile Lösungen mit hohem Informationgehalt?</p> <p>Patrick Sommer</p> <p>New & Innovative</p>	<p>10.06.2021</p> <p>Managed Detection Response Breach protection von heute und morgen</p> <p>David Mantock</p> <p>Security</p>	<p>10.06.2021</p> <p>Die Top 5 Cloud Security Wie Sie Azure und Microsoft 365 absichern</p> <p>Matthias Gessenay</p> <p>Security</p>	<p>10.06.2021</p> <p>Desaster Recovery-Szenarien Schlagen Sie dem Worstcase ein Schnippchen</p> <p>Matthias Rückemann</p> <p>Business Continuity</p>
<p>02.09.2021</p> <p>OneCloud vs. Multicloud-Strategie: Vor- und Nachteile von einem einheitlichen Ansatz</p> <p>Patrick Sommer</p> <p>New & Innovative</p>	<p>02.09.2021</p> <p>Vertrauen vs. Sicherheit am Beispiel von Zero-Trust @ SPIE (ZAS)</p> <p>David Mantock</p> <p>Security</p>	<p>02.09.2021</p> <p>Cloud Architektur Der Bauplan für Ihr Cloud-Onboarding</p> <p>Matthias Gessenay</p> <p>Governance</p>	<p>02.09.2021</p> <p>Doppelt hält besser Über das Design von redundanten Cloud Services</p> <p>Matthias Rückemann</p> <p>Business Continuity</p>
<p>04.11.2021</p> <p>News und Aktuelles von der Microsoft Ignite</p> <p>Patrick Sommer</p> <p>New & Innovative</p>	<p>04.11.2021</p> <p>Think once think twice think data Es geht immer um Daten</p> <p>David Mantock</p> <p>Security</p>	<p>04.11.2021</p> <p>Cloud Fitness Wie Sie Ihre Cloud-Infrastruktur aktuell und effizient halten</p> <p>Matthias Gessenay</p> <p>Governance</p>	<p>04.11.2021</p> <p>Das erfolgreiche Überwachen von Cloud Services</p> <p>Matthias Rückemann</p> <p>Business Continuity</p>

Security

Governance

Business Continuity

Wie setzt
man diese
praktisch um?

Cloud Governance

Theorie

Start with the three N

- Network
- Naming
- Not

Implement the Not in Policy Governance

3N

02.09.2021
Cloud Architektur
Der Bauplan für Ihr Cloud-Onboarding
Matthias Gessenay

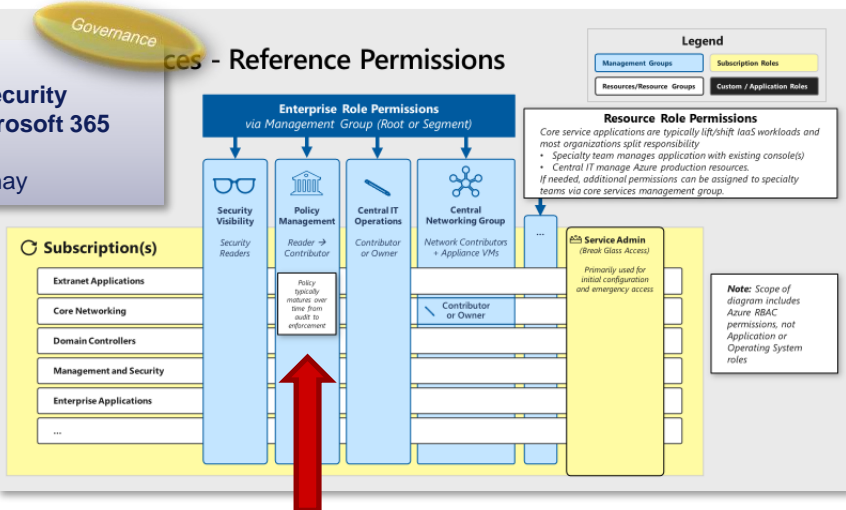


The Cloud Chapters - Teil 4 | 02.09.2021

Public



10.06.2021
Die Top 5 Cloud Security
Wie Sie Azure und Microsoft 365
absichern
Matthias Gessenay



The Cloud Chapters | 19.01.2022

Praxis

Resources

Recommendations

Resources

Recommendations

Filter for any field...

Type

Filter for any field...

Type

Showing 1 to 3 of 3 records.

Showing 1 to 3 of 3 records.

Name ↑↓

Name ↑↓

idag-dev-databricks01

idag-prod-databricks01

idag-dev-datafactory-01

idag-prod-datafactory-01

IDAG-DEV-Vnet01

IDAG-Prod-Vnet01

Naming

Not (Azure Policy)

IDAG - Location Restriction to Switzerland

Policy compliance

View definition Edit assignment Assign to another scope Delete assignment Create Remediation Task Create exemption

Essentials

Name : IDAG - Location Restriction to Switzerland

Scope : IDAG

Description : This Policy enforces the use of Switzerland Datacenter Locations

Excluded scopes : 0

Assignment ID : /providers/Microsoft.Management/managementGroups/IDAG/providers/Microsoft.Authorization/policyAssignmen...

Definition : Allowed locations

Selected Scopes

1 selected subscription

Compliance state



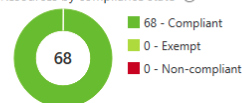
Compliant

Overall resource compliance

100%

68 out of 68

Resources by compliance state



Details

Effect Type Deny

Parent Initiative <<NONE>>

06.05.2021
**Am Ende kommt die Abrechnung:
 Wie Sie Cloud-Kosten
 unter Kontrolle behalten.**
 Matthias Gessenay

- Conduct billing administrative tasks such as paying your bill
- Manage billing access to costs
- Download cost and usage data that was used to generate your monthly invoice
- Proactively apply data analysis to your costs
- Set spending thresholds
- Identify opportunities for workload changes that can optimize your spending



The Cloud Chapters - Teil 2 | 06.05.2021

- **Gesteuertes Patching:**
 - › Mithilfe der Updateverwaltung in Azure Automation kann man Betriebssystemupdates für die virtuellen Windows- und Linux-Computer in Azure, in lokalen Umgebungen und in anderen Cloudumgebungen verwalten. Man kann den Status der verfügbaren Updates schnell auswerten und die Installation der für den Server erforderlichen Updates initiieren.
- **Automatische VM-Gastpatches:**
 - › Patches, die als *Kritisch* oder *Sicherheit* klassifiziert werden, werden automatisch heruntergeladen und auf die VM angewendet.
 - › Patches werden außerhalb der Spitzenzeiten in der Zeitzone der VM angewendet.

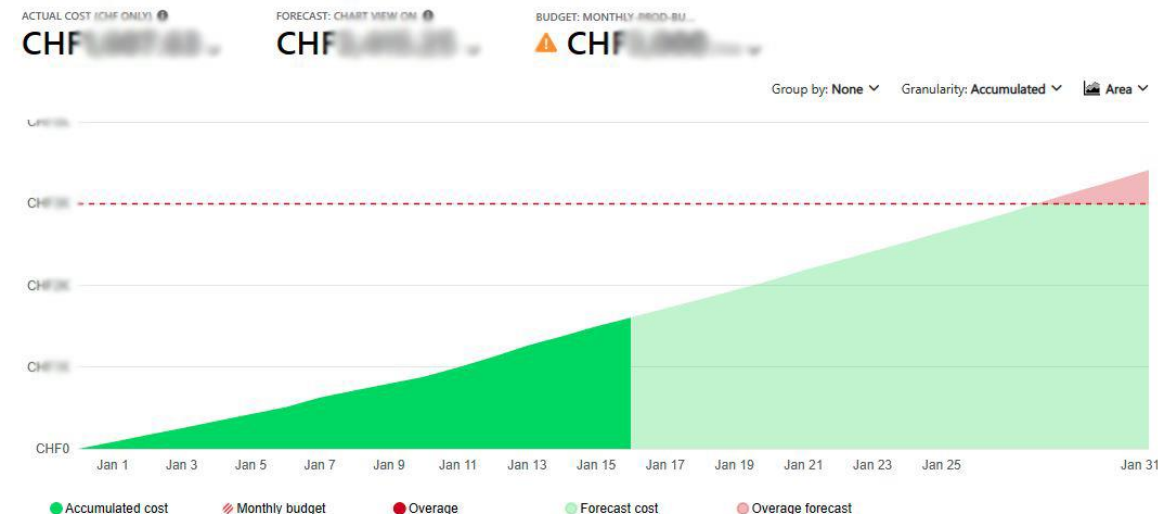


The Cloud Chapters - Teil 5 | 04.11.2021



The Cloud Chapters | 19.01.2022

Cost Management



- Azure-orchestrated VM patching


```
"osProfile": {
  "computerName": "idagadmin-prod-",
  "adminUsername": "CosoJumpHost",
  "windowsConfiguration": {
    "provisionVMAGENT": true,
    "enableAutomaticUpdates": true,
    "patchSettings": {
      "patchMode": "AutomaticByOS"
    }
  }
},
```

Windows Update

*Some settings are managed by your organization

[View configured update policies](#)



 You're up to date
Last checked: Today, 11:49 AM

Check for updates

[Change active hours](#)[View update history](#)

Advanced options



Cloud Security

Theorie

Best Practices 1 - 5



Operationalize
Secure Score for
cleaning up risk

Passwordless or
MFA for admins

Enterprise
segmentation
& Zero Trust
preparation

Enable Threat
Protection for
Azure Resources

Follow guidance
to secure your
DevOps

Best Practices 6 - 10



Assign and
Publish Roles/
Responsibilities

Choose Firewall
Strategy

Implement Web
Application
Firewalls

Choose DDoS
Mitigation for
Critical Apps

Consider
Retiring
Legacy/Classic
Technology

Governance

10.06.2021
**Die Top 5 Cloud Security
Wie Sie Azure und Microsoft 365
absichern**
Matthias Gessenay

10.06.2021
**Die Top 5 Cloud Security
Wie Sie Azure und Microsoft 365
absichern**
Matthias Gessenay

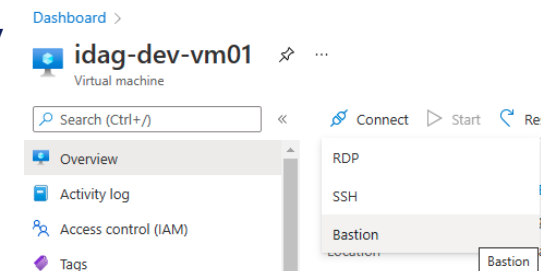
Governance

Praxis

- MFA enforced für alle Benutzer
 - › AzureAD Security Defaults
- Environment Segmentation
 - › Private Netzwerke
 - › Private Endpoints für alle PaaS Services
 - › Azure Data Gateways für Datenzugriff aus SaaS Services
 - › Zugriff nur über DevOps VM mit Azure Bastion
 - › Account Segmentation
- Builtin Azure DDoS protection
- Azure Policy

Microsoft Azure

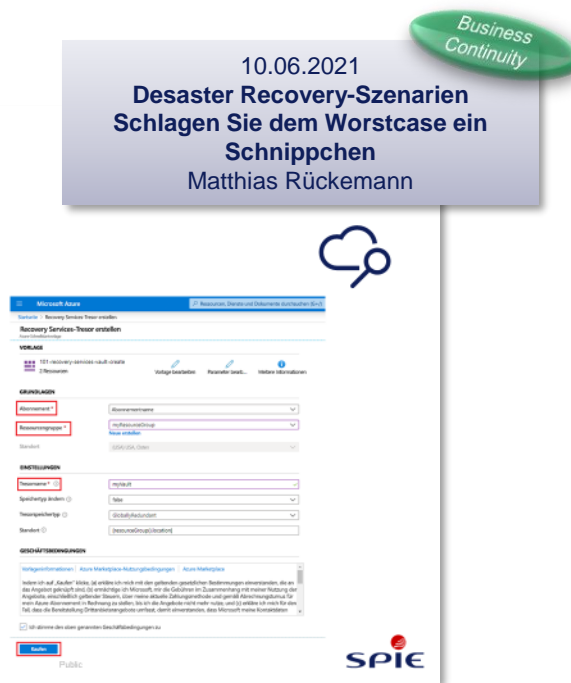
Microsoft
raphael.fae@idagadmin.ch
Anmeldeanforderung bestätigen
Öffnen Sie Ihre Microsoft Authenticator-App, und genehmigen Sie die Anmeldeanforderung.
Ich kann meine Microsoft Authenticator-App im Moment nicht verwenden.
[Weitere Informationen](#)



Praxis

- Cloud DRP: Ein Cloud-basierter DR kann von der Dateisicherung bis zum vollständigen Replikationsprozess reichen.

- › Wiederherstellung aller Infrastrukturelemente (Netzwerke, Server, Dienste) mit Templates (Zum Beispiel mit einer Azure Resource Manager-Vorlage (ARM-Vorlage, einer JSON-Datei (JavaScript Object Notation), in der die Infrastrukturen und Konfigurationen definiert sind)
- › Wiederherstellung aller Daten mithilfe vorher definierter Backup Services (Azure Backup, Veeam Backup ...)



- Datenstand wird komplett aus externen Quellen generiert => Kein Backup nötig
- Infrastruktur / Code / Visualisierungen per Azure Resource Manager Script redeployable
- Version everything: Alles was wichtig ist, liegt in einem Git Repository

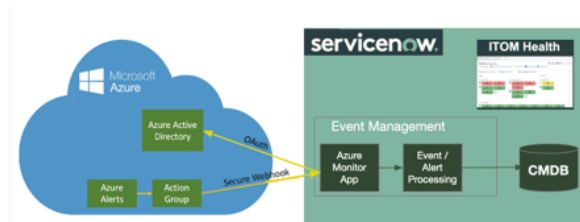
Cloud Disaster Recovery / Business Continuity

Theorie

Tips und Best Practises – Integration in ITSM Tools

● Tips und Best Practises

- › Integration nicht vergessen (zB. SNOW)



<https://docs.servicenow.com/bundle/rome-security-management/page/product/secops-integration-microsoft-exchange-online/task/ms-azure-account.html>



The Cloud Chapters - Teil 4 | 02.09.2021

04.11.2021
Das erfolgreiche Überwachen
von Cloud Services
Matthias Rückemann

Monitoring muss in ITSM-Systeme integriert werden.

- Events generieren Alerts
- Alerts generieren im ITSM System Tickets
- Tickets werden gemäss Prozess von Operatoren verarbeitet

→ Incident Management
Zur Wiederherstellung eines Services nach einem Serviceunterbruch

→ Problem Management
Zur Lösung komplexerer Probleme nach Incidents

→ Change Management
Zur Vermeidung von Incident- und Problem Tickets



Business Continuity

Praxis

Initial Ticket Collection in Teams

Ticket Management in AzureDevOps Boards

Vielen Dank!

www.spie.ch/cloudchapters



SPIE, sharing a vision for the future