Implementatie van een Air-gap oplossing met behulp van Commvault

Jean Paul Remory – SMALS

3/10/2024

Smals
ICT for society

Agenda

1. Over Smals
2. Actuele Back-Up Service
3. Actuele Bescherming
4. Wat te voorzien bij een Air-gap oplossing
5. Oplossing
6. Planning

Smals ICT for society

1. Over Smals

Vereniging van >300 openbare instellingen in België

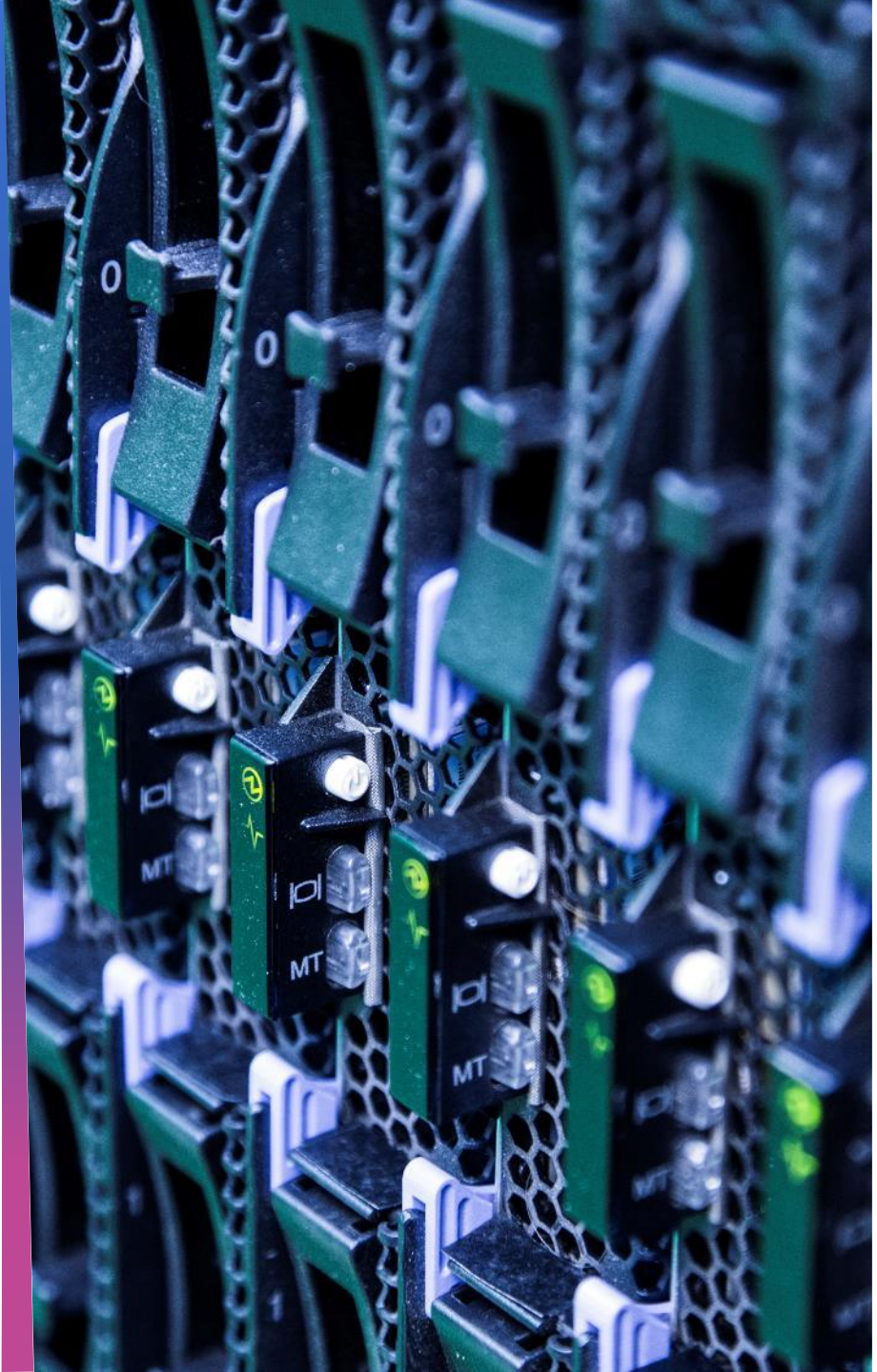
- “ICT for society” = Zuivere focus op eGovernment
- Shared services & kostendeling (non-profit)
  - Software-ontwikkeling
  - Infrastructuur & Services
  - Staffing

<u>Werkt alleen</u> voor aangesloten instellingen

- >2000 medewerkers
- >500 miljoen EUR omzet
- >50% van onze omzet gaat naar de private sector

Smals
ICT for society


sigedis
jongerenwelzijn
Vlaanderen
is zorg
actiris.brussels
de weg naar werk
BIPT
FEDRIS
hvw
OPENBARE INSTELLING VAN SOCIALE ZEKERHEID
CREG
Office national de sécurité sociale
fedasil
FEDERAAL AGENTSCHAP OPVANG ASIELZOEKERS
AGENCE FEDERALE ACCUEIL DEMANDEURS D'ASILE
BOSA
DG Digitale Transformatie
FOD Beleid en Ondersteuning
DG Transformation digitale
SPF Stratégie et Appui
POD Maatschappelijke Integratie
SPP Intégration Sociale
ibz
Federaal Instituut voor
Duurzame
Ontwikkeling
KCE
Meer dan 300 openbare instellingen …
federaal – regionaal – lokaal
eHealth
KSZ
BCSS
economie
FOD Economie, K.M.O., Middenstand en Energie
RIZIV
fagg
federaal agentschap voor geneesmiddelen en gezondheidsproducten
RVA.be
FAMIFED
Federaal agentschap
voor de kinderbijslag
Rekenhof
Cour des comptes
RJV
ONVA
VDAB
Kind & Gezin
KONINKRIJK BELGIË
Federale Overheidsdienst
Buitenlandse Zaken,
Buitenlandse Handel en
Ontwikkelingssamenwerking
Federale Politie
Federale Overheidsdienst
Sociale Zekerheid
RSZ
RIJKSDIENST
VOOR SOCIALE
ZEKERHEID

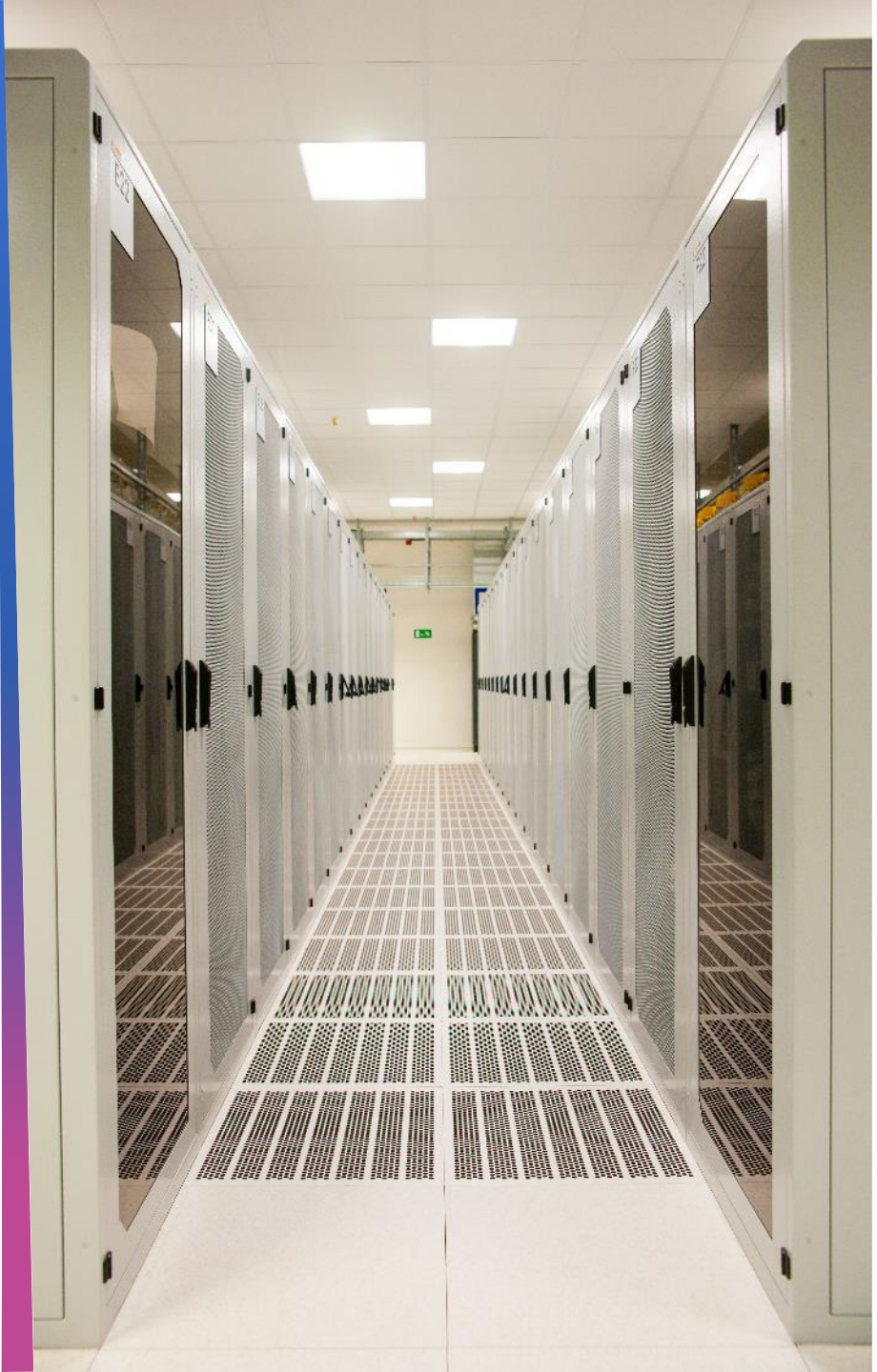


2. Actuele Backup Service

- Backup-As-A-Service laat klanten back-ups maken en bestanden terugplaatsen in geval de originele bestanden verloren gaan of beschadigd werden.
- Huidige BAAS-klanten hebben keuze uit verschillende back-up schema's.

Plan	Bewaartijd	Schema
P01	1 maand	1 maand dagelijkse backup
P02	2 maanden	2 maanden dagelijkse backup
P03	3 maanden	3 maanden dagelijkse backup
P06	6 maanden	3 maanden dagelijkse backup + 3 maanden wekelijkse backup
P12	1 jaar	3 maanden dagelijkse backup + 3 maanden wekelijkse backup + 6 maanden maandelijkse backup

Smals
ICT for society



Actuele Backup Service

- Backup as-a-Service beschikbaar in Smals-datacenters
- Klant kan kiezen tussen 'cross site' backup en 'dual site' backup
- Alle back-ups zijn online beschikbaar en kunnen op gelijk welk moment door klant teruggeplaatst worden

Smals ICT for society

3. Actuele bescherming van de Backup-omgeving

Geïmplementeerde beschermingstechnieken in Backup-omgeving:

- Backend storage in beide datacenters
- Back-up storage arrays zijn verschillend van user primary storage arrays
- Ransomware-bescherming
  - Backup platform detecteert abnormale patronen
  - Enkel het backup-platform kan wijzigingen aanbrengen op back-up data
- End-to-end encryptie
- Keuze tussen single backup copy (cross-side) en dubbele backup copy (dual site)

Smals ICT for society

Actuele bescherming van de Backup-omgeving

Wat is er beschermd ?

- Data loss of “corrupte” data op client server
- Site disaster
  - Voor single backup : alle backup-kopieën op de verloren site zijn mogelijk verloren
  - Voor dubbele backup: 1 kopie blijft altijd ter beschikking
- Ransomware-infectie
  - Bescherming indien backup data besmet is binnen retentieperiode

Smals ICT for society

Actuele bescherming van de Backup Omgeving

Wat is NIET beschermd :

Risico op ontoegankelijk maken van backups in productie

- Ransomware-infectie van backup ouder dan de retentie periode
- Risico op ontoegankelijk maken van backups in productie (infectie van backup productieomgeving)

Een oplossing om dit risico te minimaliseren en mogelijk herstel te bieden is **een Air-gap kopie** te voorzien:

“Air-Gap-kopie is een kopie die volledig geïsoleerd is van het productienetwerk”

Smals ICT for society

4. Wat te voorzien bij een Air-gap-oplossing?

Maximaal beveiligde Air-gap-omgeving kunnen we realiseren door :

- Maximaal afscheiden van opslag door deconnectie en/of logisch isoleren van productienetwerk
- Beheersomgeving van de Air-gap-oplossing maximaal isoleren
- Maximaal desactiveren van toegangen op Air-gap-toestellen in de geïsoleerde omgeving
- Strikt rol-gebaseerde toegangscontrole + MFA toegang op Air-gap omgeving (en productie)
- Encryptie van alle gegevens
- Ander type storage met optie WORM-functionaliteit
- Voorzien van Clean Room om backup te kunnen terugplaatsen en ontsmetten

Smals ICT for society

Wat te voorzien bij een Air-gap-oplossing?

Mogelijke alternatieven voor het medium waarop de kopieën gezet worden :

Air-gap to connected remote disk	
PRO	CON
• Cost? • In existing environment • Known technology	• How to realise 100% isolation of existing network
Cloud Storage	
PRO	CON
• Flexible (capacity) • Security? Distiction in client offering between second copy and air-gap copy	• Cost • Connectivity • Out of controlled perimeter • 100% isolation possible?
Tape	
PRO	CON
• Cost • 100% offline	• New processes involving people interventions if no robot

Smals ICT for society

5. De gebouwde oplossing

- 34 mogelijke aanvalsvectoren geëvalueerd bij architectuurontwerp
- Gekozen architectuur zal maximum aan vectoren neutraliseren
- Aparte omgeving ondergebracht in derde datacenter
- Creatie van derde – geïsoleerde – backup-omgeving
- Connectiviteit beheerd door power controller, die verbindingen aan / af zet
- Design samen met externe specialisten en interne security architecten van Smals

6. Planning

- Oplossing beschikbaar voor testen eind dit jaar
- Volledige productiebeschikbaarheid en uitbereiding productieomgeving : vanaf 2025

Smals ICT for society