Technologie IBM pro bezpečný cloud

Petr Leština
petr_lestina@cz.ibm.com

Agenda

RedHat a IBM a pokračující spolupráce

Bezpečnost pohledem *architektury*, *principů* a *standardů*

Zabezpečení dat: během přenosu & ukládání

Bezpečnostní monitoring

Nejčastější dotazy klientů spojených s ochranou dat v cloudu.

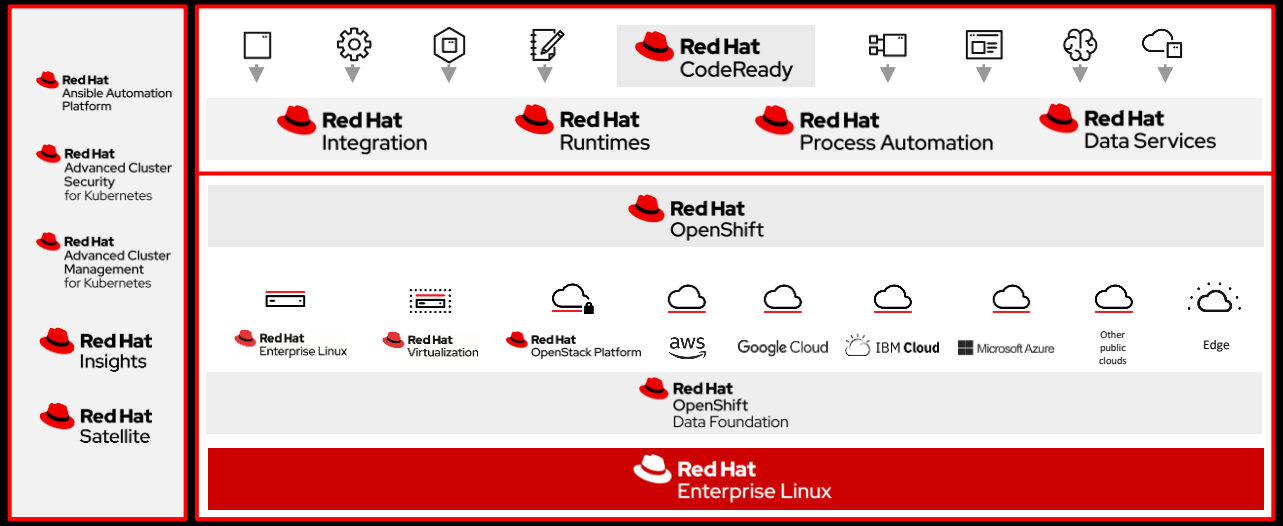
IBM **Cloud**

Strategické směry pro rok 2022

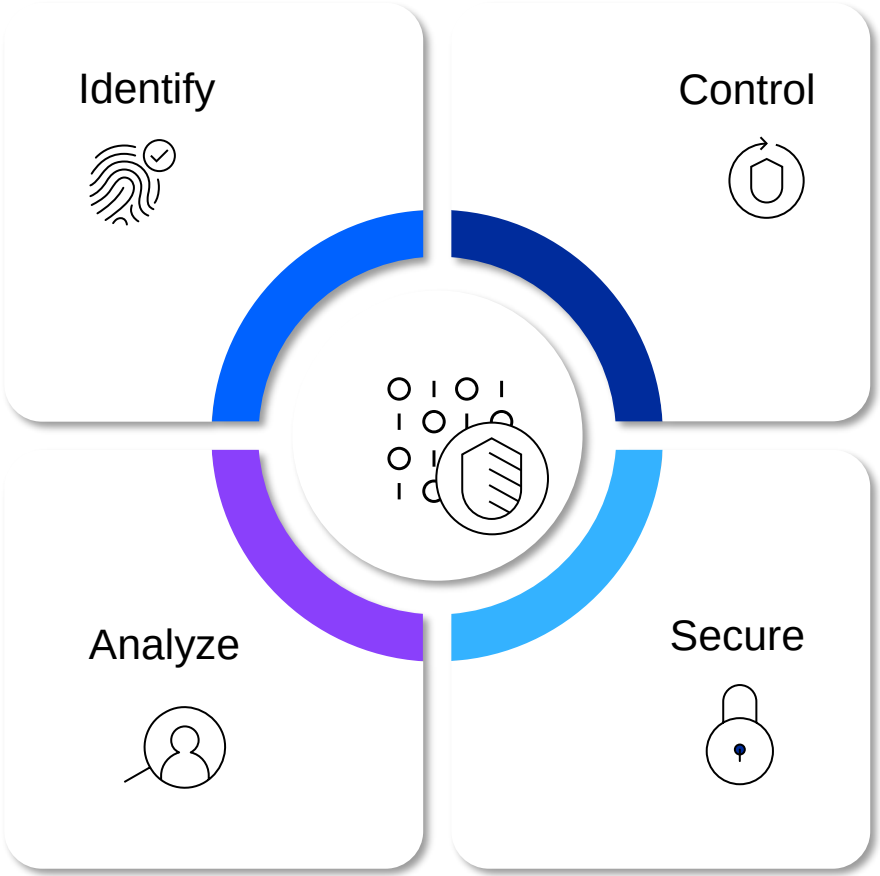
1. AI – Umělá inteligence
2. Cloud Native řešení
3. Hybridní cloud
4. Multi-cloud
5. Bezpečnost

IBM & RedHat v roce 2022

- Zachován operační model
- IBM vlastní RedHat, obě společnosti však fungují nezávisle!
- Platí globálně i v ČR
- Podpora pro OpenSource jako takový zůstává
- Multi-Cloud & Multi-vendor strategie



Bezpečnostní přístup: *Zero Trust*



↳ **Ověření** uživatele

↳ **Autorizace** přístupu

↳ Ke **službám** a **datům**

↳ V rámci **privilegií**

IBM Cloud Security Framework – koncepční rámec

Security Policy | Security Controls | Risk Management | Audit & Compliance

Security on the Cloud – Bring your own security

Identity & Access
- Identity Governance
- Risk Based Access

Application Security
- App Scanning
- Threat Protection

Data Security
- Activity Monitoring
- Classification & Governance

Infrastructure Security
- Endpoint management
- Network Protection

Security Intelligence
- Security Monitoring
- Threat Management
- Incident Response

Security in the Cloud – Integrated Security Services in public cloud

Security Services

Security Visibility & Management
- Security & Compliance Posture
- Threat Intelligence
- Policy Management & Orchestration

Identity & Access
- Identity
- Authentication & Federation
- Access Control

Application Security
- Vulnerability management
- App threat Protection
- Security Scanning

Data Security
- Data Encryption
- Key Management
- Data Access

Secure Platform

Secure Network
- Virtual Private Cloud
- Network ACLs
- Security Groups
- VPN
- DDoS mitigation

Secure Compute
- Containers
- Virtualization
- Servers
- Compute Integrity
- Compute Isolation
- Runtime Encryption

Secure Storage
- Storage Encryption
- Storage Isolation
- Hardware Security Modules

Physical Security

Data center security | Access & Surveillance | Operational Controls | Personnel & Training

Bezpečnostní principy

1 **Klient vždy zná umístění svých dat**

Lokace datacenter je k dispozici v ISO 27k certifikátech

2 **Zabezpečení dat určuje klient**

BYOK, KYOK, šifrování dat, AES 256

3 **IBM nepoužívá klienská data**

Pro žádné účely (trénování Watsona, Vylepšení produktů apod.)

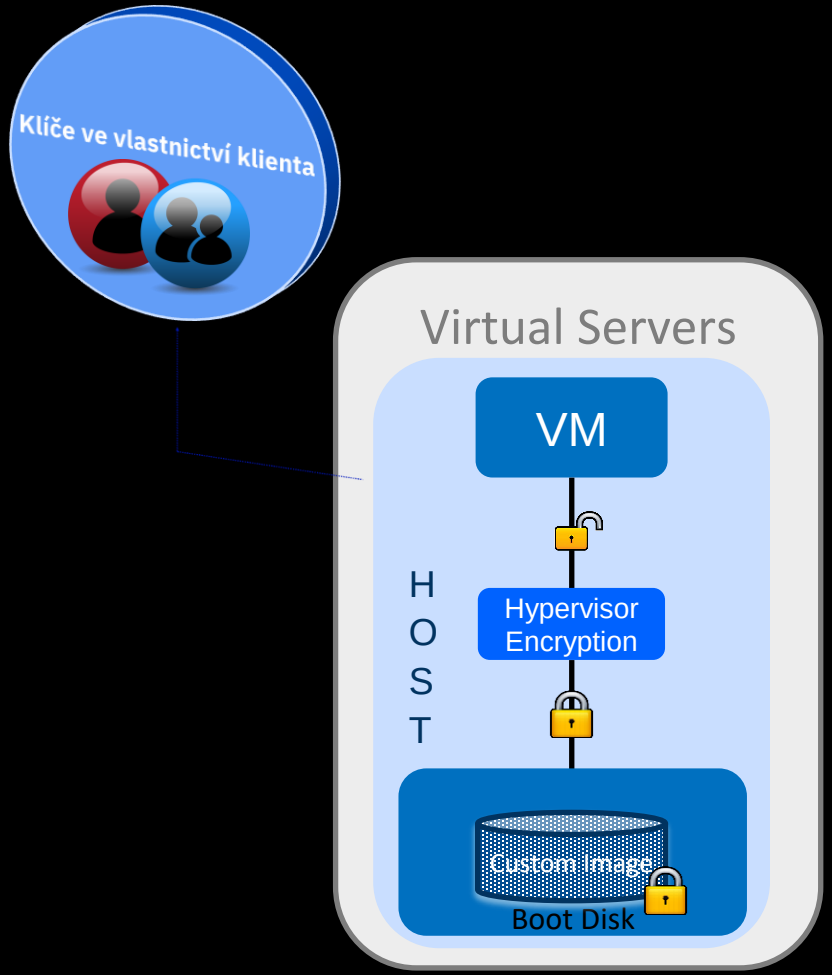
Šifrování a zabezpečení dat

Během přenosu (Data-In-Transit)

- HTTPS, SSL, a TLS při přenosu po internetu
- VPC/VPN gateway zajistí IPsec site-to-site link
- IBM Direct Link pro privátní linku
- Security Gateway
  - Juniper vSRX
  - ATT Virtual Router Appliance

Ukládání (Data-At-Rest)

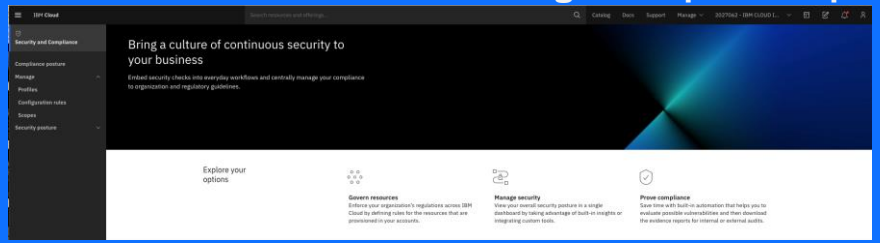
- Klient určuje mechanismus šifrování, s technologiemi Hytrust a BYOK/KYOK
- OS image šifrovaná BYOK/KYOK
- IBM Cloud hardware security modules (HSMs)
- File/Block Storage šifrovaná standardně AES-256
- Výpočetní výkon zabezpečený pomocí Intel TPM/TXT

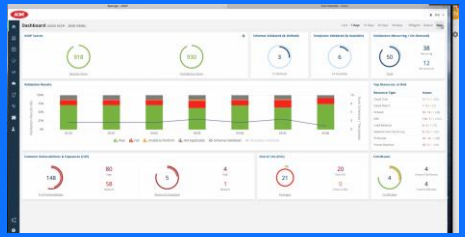


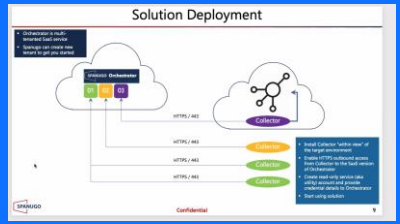
Bezpečnostní monitoring v Cloudu

IBM Cloud Security and Compliance Center

Integrované prostředí pro správu a bezúečnostní monitoring

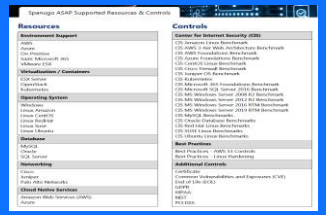






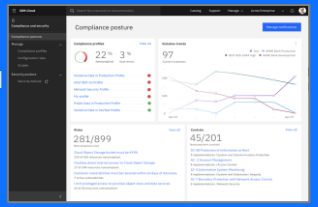
Bezpečnostní pravidla a principy

Bezpečnostní prinipy založené na NIST based control assessments.



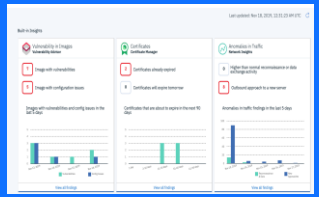
Řízení bezpečnostních konfigurací

Správa a řízení bezpečnostních parametrů pro IBM Cloud public services



Bezpečnostní náhled

Visualizace a náhled na zranitelnosti network & activity behavior, expirace certifikátů



IBM Cloud Kubernetes Service

kubernetes

Red Hat OpenShift

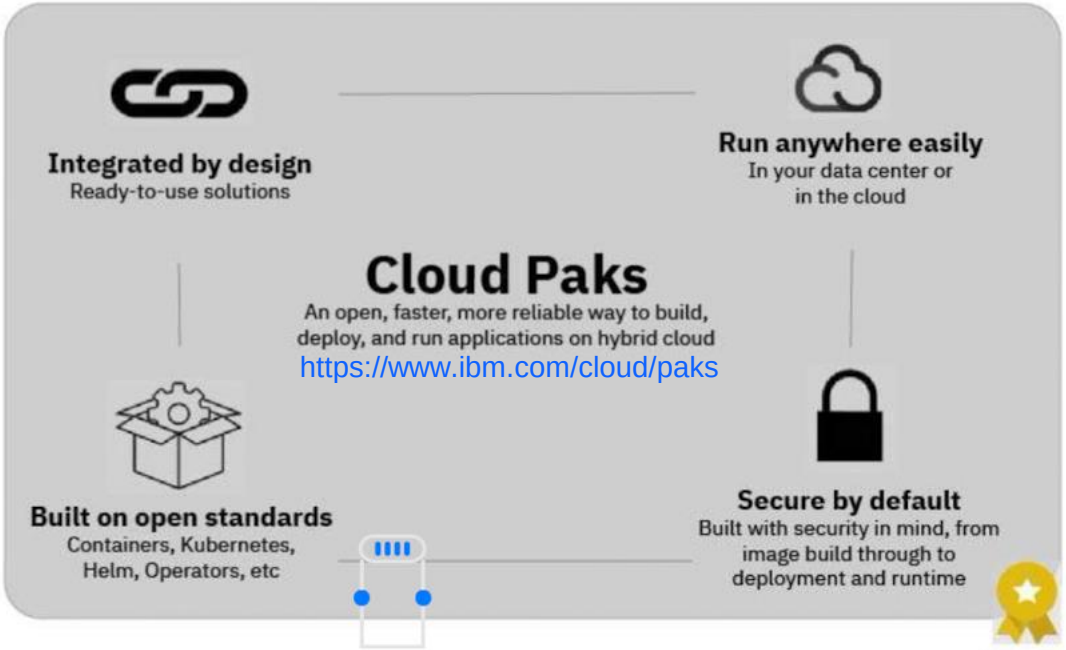
Je služba typu "**managed service"** umožňující intuitivní konfiguraci, provoz a monitoring **Kubernetes** clusterů. Zahrnuje prostředky pro **bezpečnost a izolaci** provozu **cloud-native aplikací**, rozšiřitelné o monitoring, DevOps, Analytiku i nástroje pro IoT, **AI včetně Watsona.** K dispozici v 6 regionech IBM, worldwide, celkem ve více než **30+ datacentrech.**

Více na: www.ibm.com/cloud/container-service

IBM CloudPak představuje *„kontejnerizované“* IBM produkty v prostředí Redhat OpenShiftu

- Cloud Pak for *Data*
- Cloud Pak for *Security*
- Cloud Pak for *Business Automation*
- Cloud Pak for *Watson AIOps*
- Cloud Pak for *Integration*
- Cloud Pak for *Network Automation*
- CloudPak *System*

IBM Cloud Paks



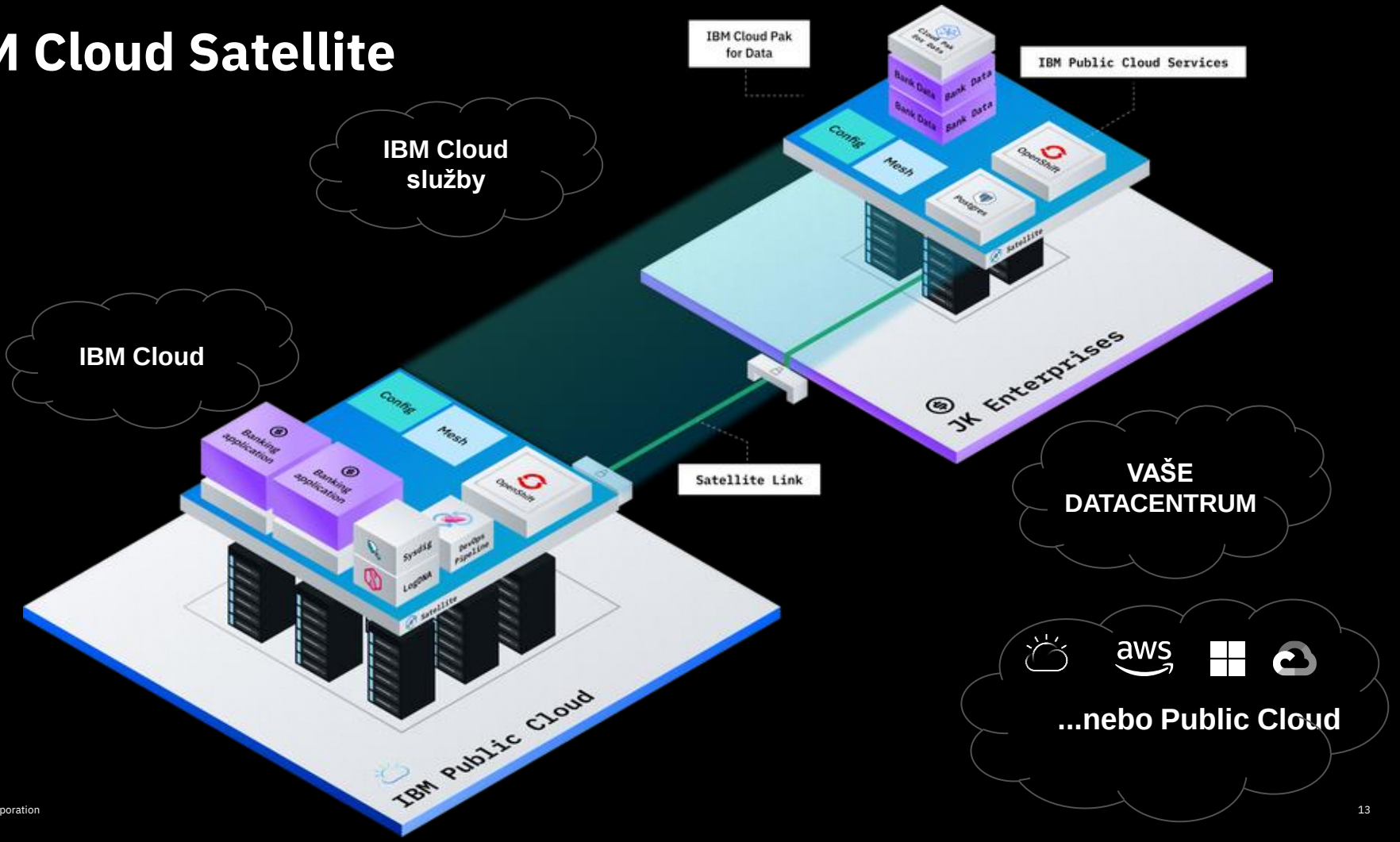
Red Hat OpenShift

IBM Cloud Paks využívají Red Hat Kubernetes OpenShift Container Platform

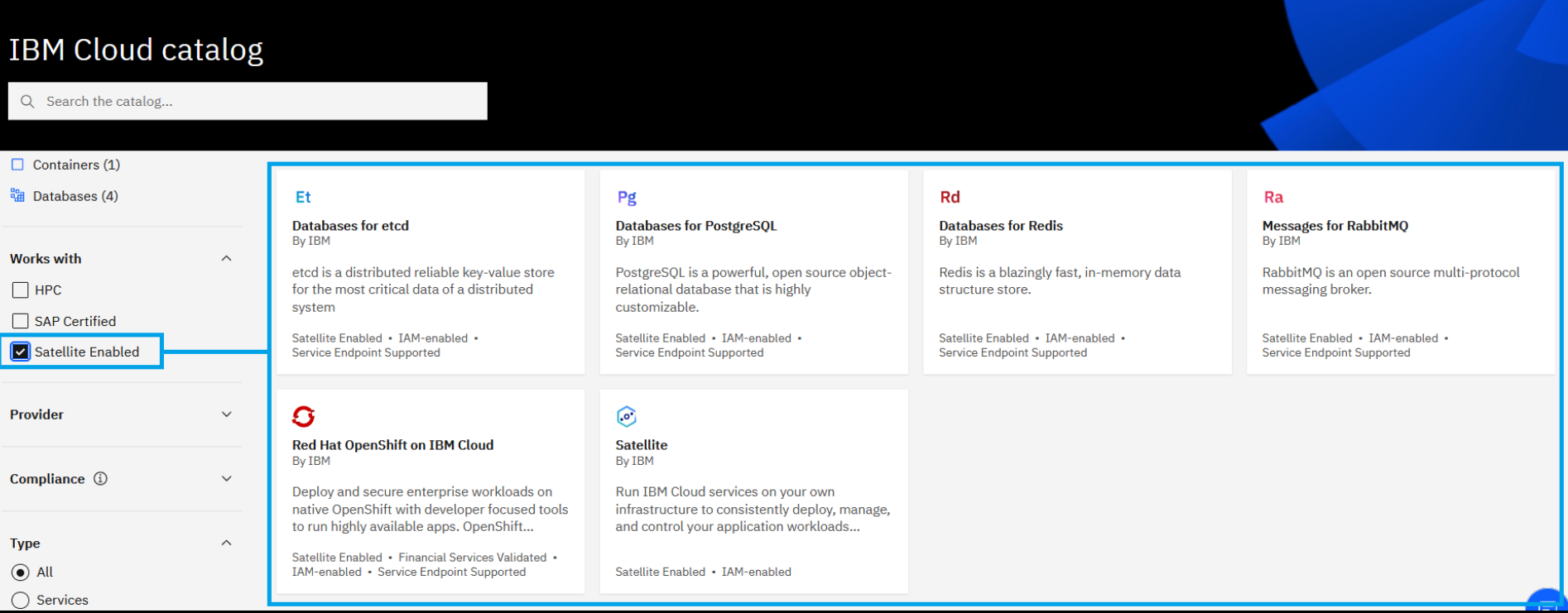
Co je **IBM Cloud Satellite** ?

IBM Cloud služba provozovaná ve Vašem datacentru, implementovaná v režimu as-a-service a řízená z prostředí public cloudu.

IBM Cloud Satellite



IBM Cloud Services v Satellit*u*



IBM Cloud

aws

Azure

IBM Cloud Satellite

Vše co potřebujete je **Linux**ová infrastruktura, **IBM** zajistí to ostatní

IBM Cloud certifikáty

https://www.ibm.com/cloud/compliance

IBM Cloud a základní standardy

IBM Cloud Security Policy

Based on ISO27001 **NIST SP800-53**

Průmyslové a regionální certifikáty

SOC1, SOC2, SOC3

Germany

DoD DISA IL-2

ENS High Spain

EU Model Clauses IBM Data Processing Addendum (DPA)

FedRAMP** High

Hébergeurs de Données de Santé (HDS) Health Data Hosting

MTCS L3

Australia

ISO/IEC 9001

ISO/IEC 27001

ISO/IEC 27017

ISO/IEC 27018

ISO 31000 Risk-Management

PCI DSS Level 1

Průmyslové a odvětvové certifikáty pro banky, telco, zdravotnictví a další segmenty

Germany – Federal Financial Supervisory Authority

STAR Level 1

Self Assessment

Federal Information Security Modernization Act

FISMA

GDPR

ITAR

My Number Act Japan

EU-US

Aktuální certifikáty jsou on-line na webu a lze je zdarma downloadovat

Nejčastější dotazy od klientů...

IBM Cloud

Otázka #1: *„Kde jsou moje data? Mohu znát fyzickou adresu datacentra cloudového poskytovatele? Lze jej auditovat?“*

Otázka #2: *„Jak je to se šifrováním dat na sdíleném úložišti typu Block/NFS File Storage? Co se stane s poškozenými disky a jak jsou likvidovány?*

Otázka #3: *„Jak je to s EXIT strategií? Mohu si data z cloudu kdykoli odnést/exportovat a provoz kdykoli ukončit?*

SCAN ME

IBM

IBM Cloud