

Maximo EAM to MAS



OpenShift Platform Options

Ben Poston
IBM Cloud Modernization SME
postonb@us.ibm.com

July 2024



A Modernized Software Product Requires a Modern Platform

Example: Maximo Application Suite on Red Hat OpenShift

Manage

Intelligent
Asset
Management



Monitor

Monitor and
Detect
Anomalies



Health

360 View of
Assets



Predict

Predictive
Failures



Visual Inspection

AI-Powered
Insights



Schedule

Schedule
Work and
Resources



Mobile

Technician
Work
Execution



Assist

Prescriptive
Assistance



Control

ITIL Based
Technology
Service
Management



IBM Cloud Pak for Data | IBM Watson Studio | IBM Watson ML

IBM Cloud Security and Compliance Center Workload Protection



Infrastructure Independent
Common Operating Environment



We must upgrade to MAS but have challenges:

We have databases and applications on-prem that must integrate with MAS

We don't want to migrate everything to cloud



We have regulatory or latency requirements requiring data to stay on-prem

Not all data can go to the cloud. Regulatory or network latency requirements force application to stay on-prem



Need to deploy and be in production quickly

We don't have months to spend on building and testing a new containers platform




No OpenShift Skills (or not enough)

Container skills are in high demand, tough to find (especially in small markets) and can be very expensive



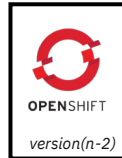
Common Deployment Options

Deployment	Procure	Provision & Operate	Client Benefits
On Premises Customer Managed	Client purchases software from IBM, partner or ISV Client provides data center and infrastructure	Client provisions, manages, and operates full stack	<ul style="list-style-type: none"> • Maximum operational flexibility
SaaS ISV Managed	Client purchases software as a service including infrastructure, hosting, platform and software.	Client logs in and uses immediately	<ul style="list-style-type: none"> • Reduced time-to-value • No data center, hosting, infrastructure or maintenance • Allows clients to focus on business priorities
Hyperscalers Customer Managed Software with Optional Managed OpenShift	BYOL or Marketplace Software Purchase Infrastructure-as-a-service by cloud provider Optional platform-as-a-service provided by cloud provider	Provision IaaS and/or OpenShift on Hyperscalers' cloud Client manages and operates both software and infrastructure with option for managed OpenShift platform	<ul style="list-style-type: none"> • Simplifies procurement and deployment • Client can focus on application and not platform • OpenShift platform as a service does not require client labor or skills for management
Custom Managed Service	Client procures partial or full stack service from a managed service provider	MSP provisions, manages and operates Client's partial or full stack environment on prem, in a co-location facility, or in any cloud	<ul style="list-style-type: none"> • Option for full stack management • Allows clients to focus on business priorities • Can leverage IBM Cloud Satellite and ROKS for speed and lower costs
On Premises IBM Cloud Satellite w/ Managed OpenShift Service 	Client purchases software from IBM, partner or ISV Client provides infrastructure or partner provided Platform services including IBM Cloud Satellite and managed Red Hat OpenShift via subscription	Client provisions and manages infrastructure & application, IBM manages platform including OpenShift & SCC Workload Protection with optional installation services	<ul style="list-style-type: none"> • IBM manages the OpenShift platform across on prem and hyperscalers in a hybrid or multi cloud topology • Lower cost than DIY • Cloud benefits in client data center • Consistent OpenShift operational experience across hybrid and multi cloud • Easily identify vulnerabilities, check compliance, block runtime threats and respond to incidents faster



“ Because we use **Red Hat OpenShift on IBM Cloud**, we spend **less time managing infrastructure**, and we have **more time to listen to business needs** and **develop new applications to accommodate them.**”

Herwig Bogaert
Senior System Engineer, meemoo



First to market
for 4 years
and counting!

Fully automated. As-a-service. Extend anywhere.

Key Capabilities



OpenShift experience built on Kubernetes

Use the OpenShift tools and APIs you already know for a single, consistent experience, even when working across hybrid environments or different cloud providers.



Heightened cluster and app security

IBM provides security features to protect your cluster infrastructure, isolate your compute resources, encrypt data, and ensure security compliance in your container deployments. Further, OpenShift sets up strict Security Context Constraints for greater pod security by default.



Worldwide, continuous availability

Deploy and scale workloads across the globe in all IBM Cloud multizone regions. OpenShift clusters include a managed master that is automatically spread across zones within the region for high availability.



Integrated OpenShift catalog

Quickly set up a CI/CD with Jenkins or deploy a variety of apps in a guided experience that's fully integrated into your OpenShift cluster.



Innovation with watsonx, Cloud Paks, & the IBM Cloud platform

Easily integrate generative AI with Watson APIs to extend the power of your apps. Access the IBM middleware in IBM Cloud Paks from within the scalable public cloud. You also get built-in services for monitoring, logging, load-balancing, storage, and security to help you manage an app's lifecycle.

Up to 99.99% SLA

24x7 SRE global support

Secure by default

Keep Your Own Key (KYOK)
with Hyper Protect Crypto
Services, FIPS 140-2 Level 4
Certified

Highly-compliant

Cluster Autoscaler

Worldwide SZRs & MZRs
& extend **on-prem**, at the **edge**,
or public cloud environments
with **IBM Cloud Satellite**

Workload **Security & Compliance**
managed with SCC Workload
Protection

Seamless GPU support

Public Slack workspace



Add-on Capabilities



OpenShift Data Foundation

Manage data, stay consistent everywhere, handle application needs.



OpenShift AI

Build, deploy, and manage AI-enabled applications.



Tekton

Create Kubernetes-native CI/CD pipelines with maximum speed and flexibility.

Our Clients



OpenShift Day 2 Responsibilities

IBM enables you to focus on your core business, not platform management

Responsibilities:

- Customer
- IBM
- Shared

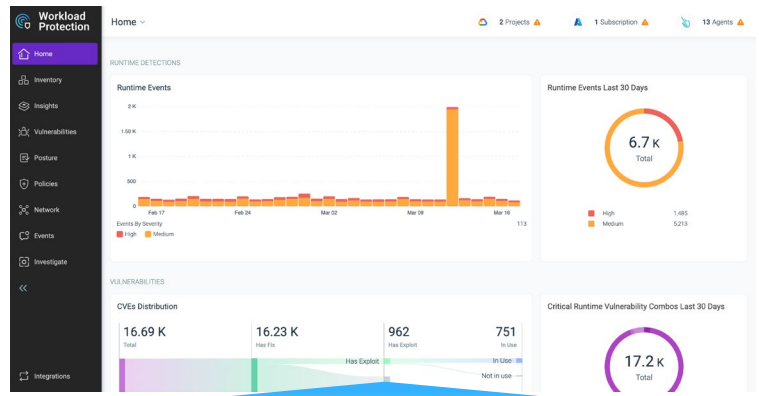
	DIY	With ROKS
Create and configure OpenShift clusters, including geographic deployment options	●	●
Integrate CI/CD pipeline to appropriate endpoints & manage your applications	●	●
Automated provisioning and configuration of Infrastructure (compute, network and storage)	●	●
Automated installation and configuration of OpenShift , including HA cross zone configuration	●	●
Automatic upgrades of all components (operating system, OpenShift components, and in cluster services)	●	●
Security patch management for OS and OpenShift	●	●
Automatic failure recovery for OpenShift components and worker nodes	●	●
Automatic scaling of OpenShift configuration	●	●
Automatic backups of core OpenShift ETCD data	●	●
Built in integration with cloud platform - monitoring, logging, KeyProtect, IAM, ActivityTracker, Storage, COS, Security Advisor, Service Catalog, Container Registry and Vulnerability Advisor	●	●
Built in Load Balancer, VPN, Proxy, Network edge nodes, Private Clusters and VPC capabilities	●	●
Built-in Security including image signing , image deployment enforcement, and hardware trust	●	●
24/7 global SRE team to maintain the health of the environment and help with OpenShift	●	●
Global SRE has deep experience and skill in IBM Cloud Infrastructure, Kubernetes and OpenShift, resulting in much faster problem resolution	●	●
Automatic compliance for your OpenShift environment (HIPAA, PCI, SOC1, SOC2, SOC3, ISO)	●	●
Capacity expansion through a single click	●	●
Automatic multi-zone deployment in MZRs , including integration with CIS to do cross zone traffic routing	●	●
Automatic Operating System performance tuning and security hardening	●	●

IBM Security and Compliance Center (SCC)

Cloud-Native Application Protection Platform (CNAPP) for hybrid multicloud environments



Overall Leader for CNAPP
KuppingerCole 2024
Leadership Compass



Posture Management (CSPM)



Permission Management (CIEM)



Vulnerability Management (CWPP)



Threat Detection & Response (CDR & EDR)

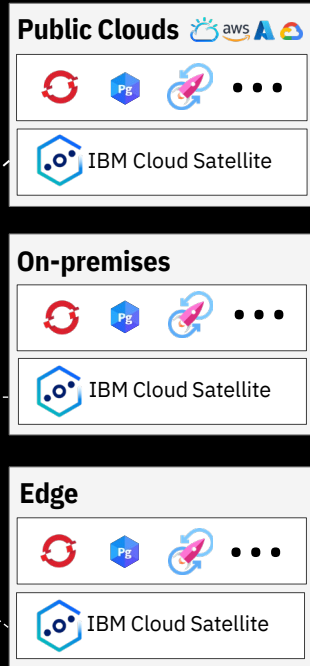


Automation & Integration

Across hybrid multicloud environments

Supported environments include: IBM Cloud, IBM Cloud Satellite, OpenShift, AWS, Azure, Google Cloud, VMware, IBM PowerVS, and On-premises.

Deployment Options with IBM Cloud Satellite



IBM Cloud Satellite

Workloads located where you need them

Location

Client-controlled infrastructure outside of IBM Cloud data centers

Client manages their hosts (infrastructure) within a location

Flexibility

Run app where it makes sense

For regulated workloads, sovereignty & data gravity concerns, migrations, edge platforms, low latency

Flexible infrastructure options including bring your own – Install on HyperV, Vmware, bare metal, any cloud, integrated appliances

Control

Auditable inventory of all network connections and traffic

Central observability (monitoring, security & compliance posture management from a single pane of glass with SCC Workload Protection)

IBM Cloud for Financial Services Validated

Satellite Reference Architecture for FS Cloud

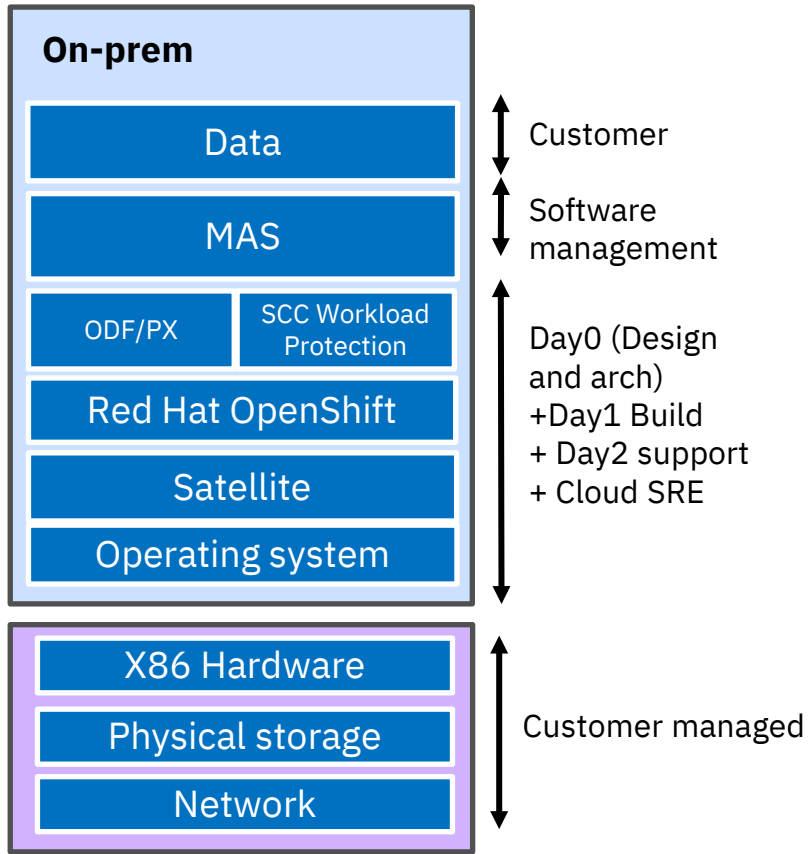
Shared responsibility model for end-user support

IBM :

- Provides support for OS and above
- Includes lifecycle management of managed platform aaS
 - Red Hat OpenShift
 - Satellite
 - Storage - Red Hat OpenShift Data Foundation (ODF)
- IBM Cloud SRE support to help debug platform related problems
- Maximo software support
- **Optional** – Full stack build and Day2 support from OS to MAS software as single point of support avoiding silos (IBM Consulting)
- **Optional** - Architectural services for DR and multi-cluster/location design(Expert labs)

Customer:

- Owns and manages infrastructure
 - Hardware
 - Storage
 - Network
- Owns and manages application integration to other backend systems
- Respond to end user issues and initiate troubleshooting
 - Work with IBM Cloud SRE teams to debug platform issues



MAS Deployment Decisions

On-Premises or Cloud/Hosted

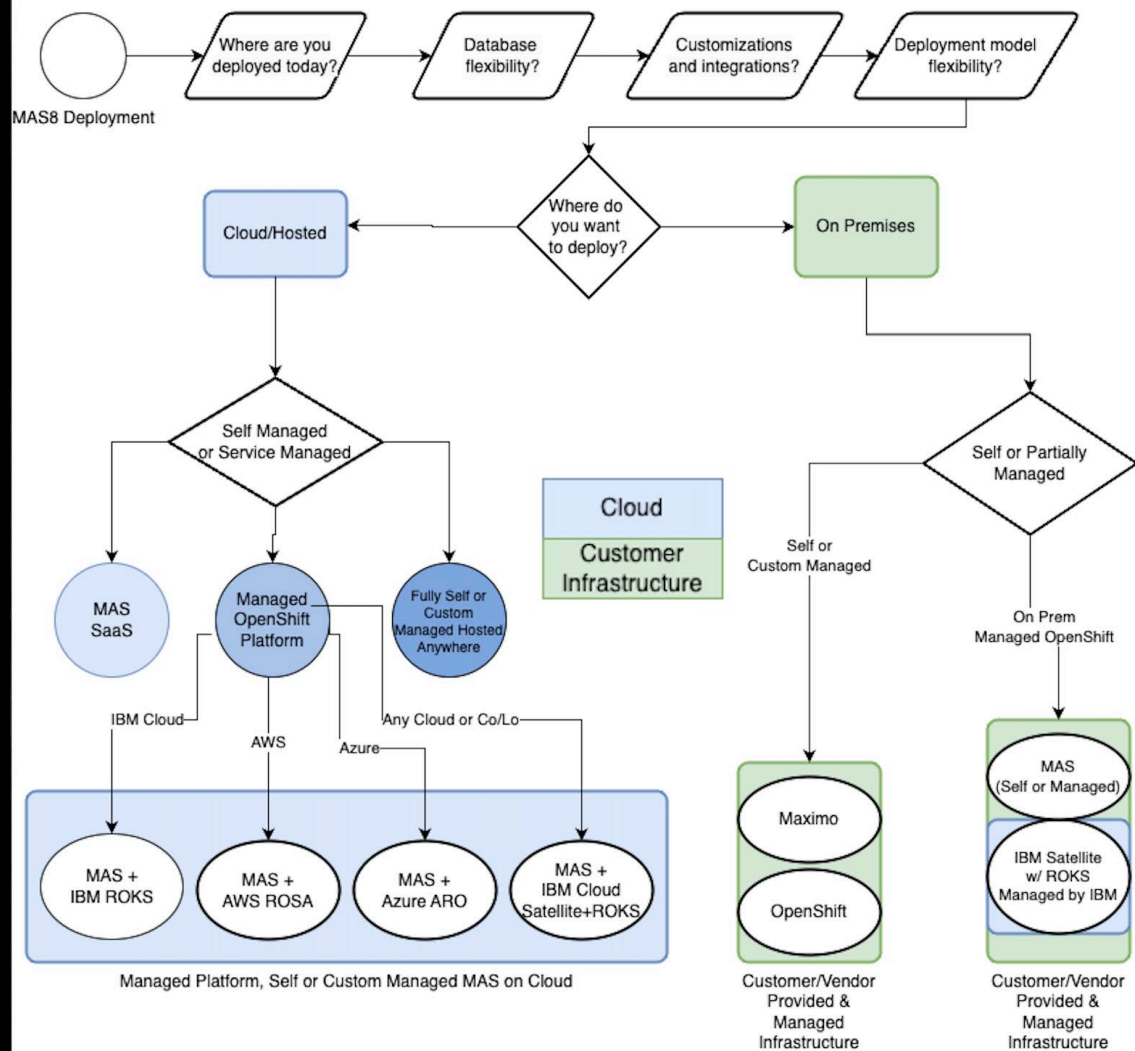
Fully managed, partially managed, managed OpenShift

Hybrid Cloud or Multi Cloud

IBM Cloud Satellite with ROKS can:

Bring managed OpenShift to your data center and/or other clouds with IBM Cloud Satellite

Simplify Hybrid and/or Multi Cloud deploy and management complexity including single pane management

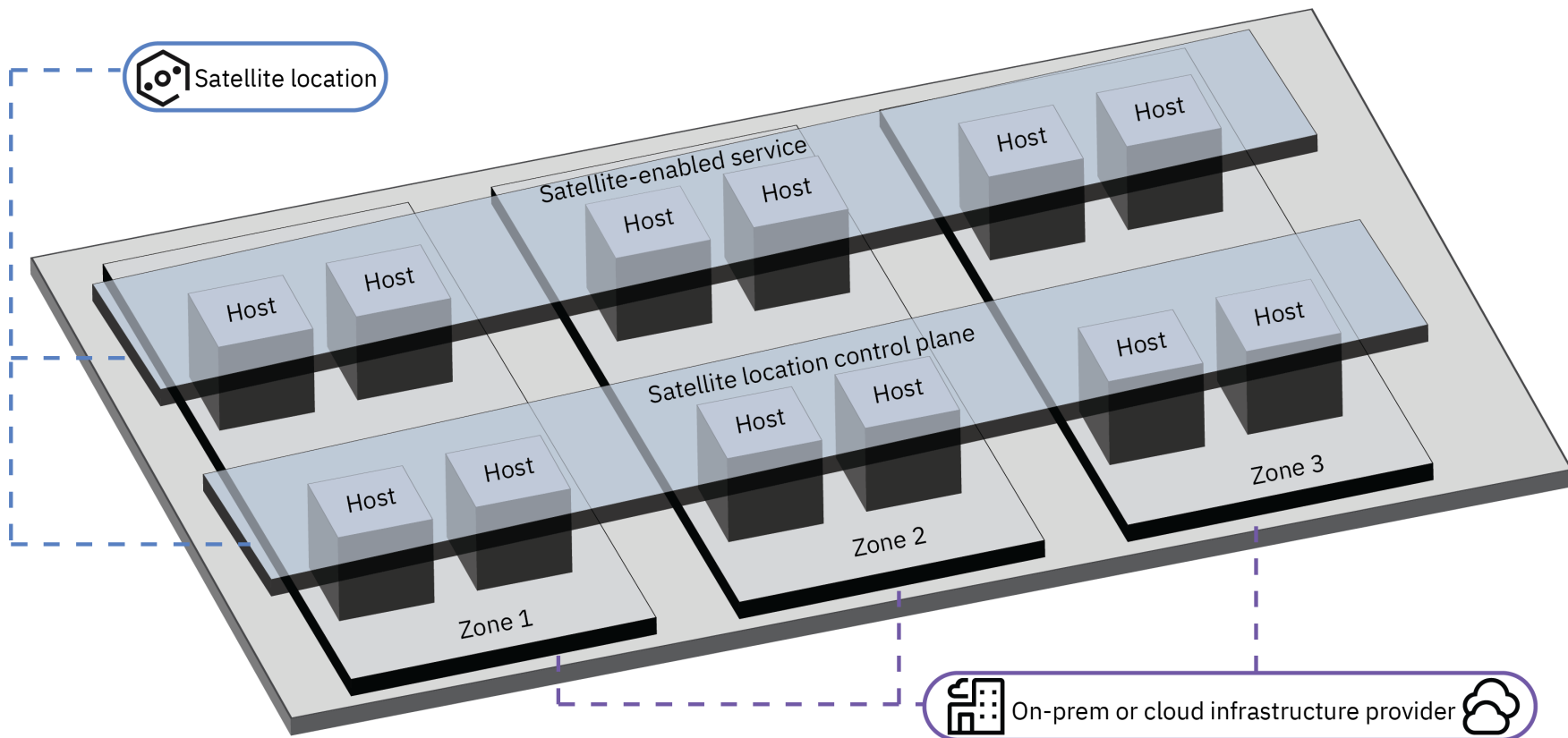


**Why ROKS Hosted
in the IBM Cloud?**

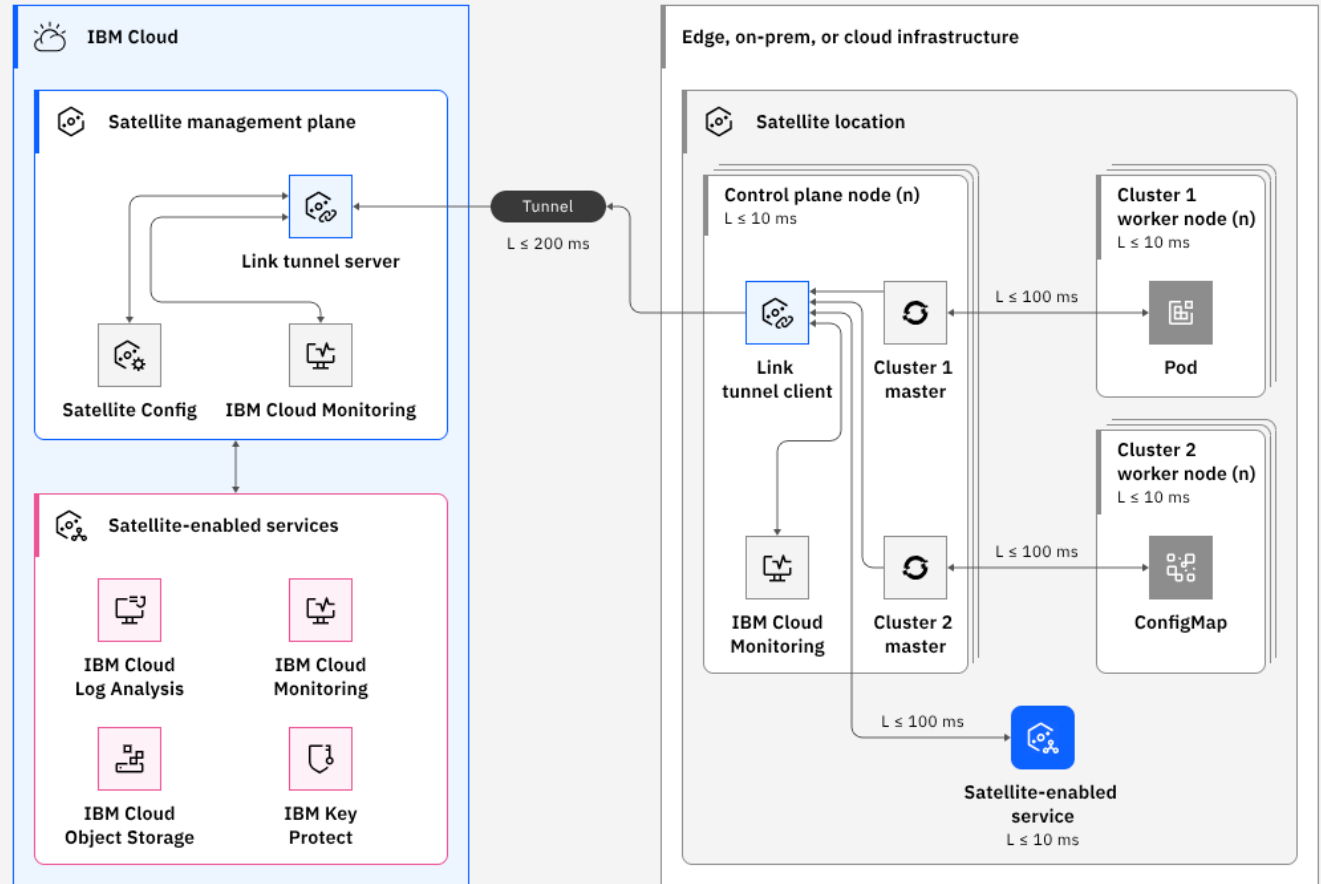
Backup

Satellite Architecture

Multi-Zone HA Architecture Built on Kubernetes

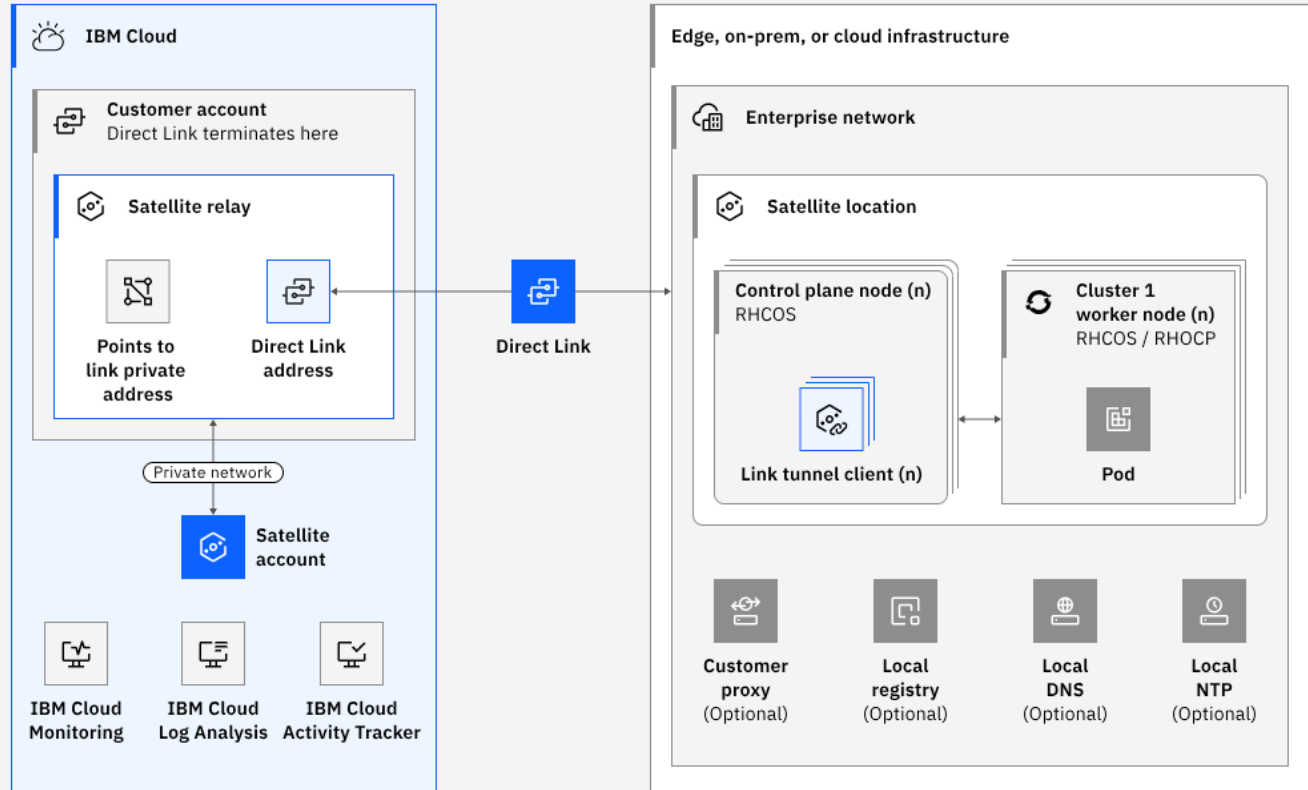


Satellite Architecture



Logical node
 Prescribed node
 Multiple instances, where $n \geq 1$
L = latency requirement

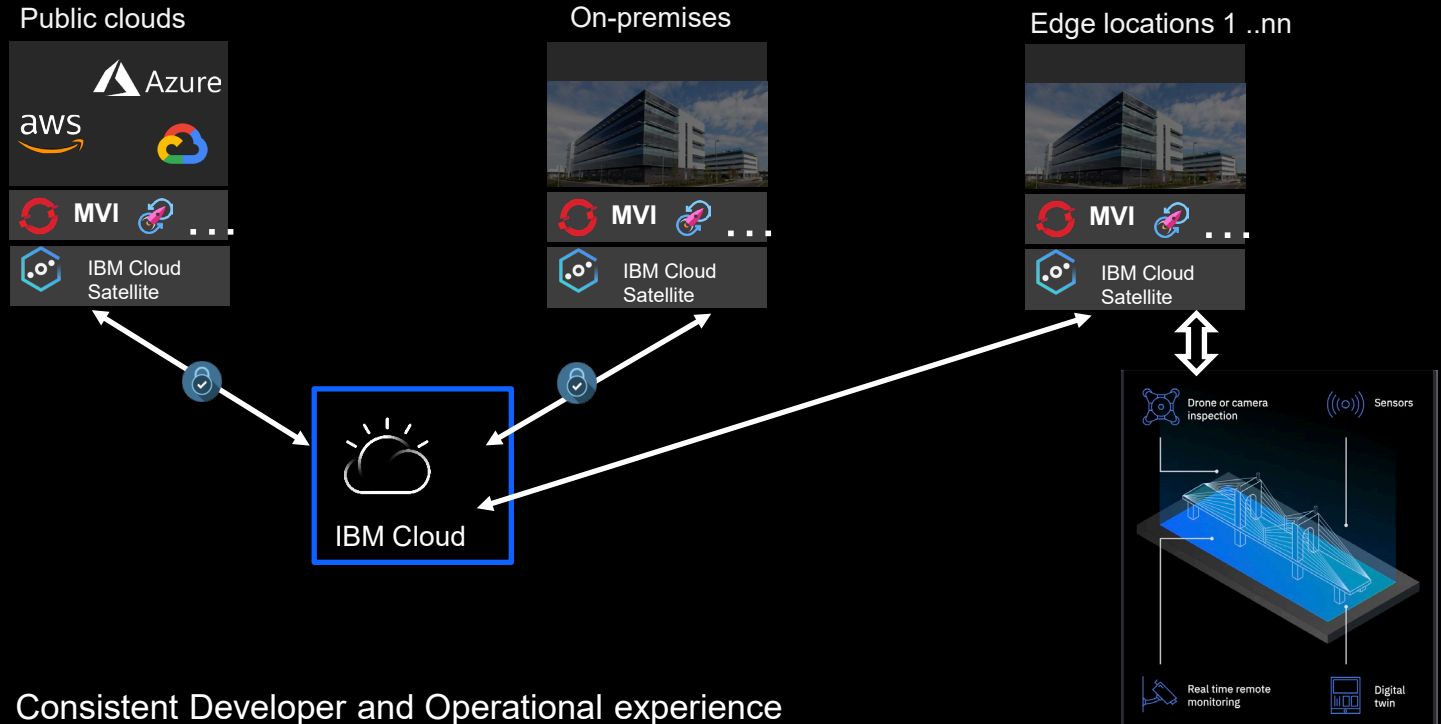
Satellite Architecture with Direct Link



Logical node Prescribed node Multiple instances, where $n \geq 1$

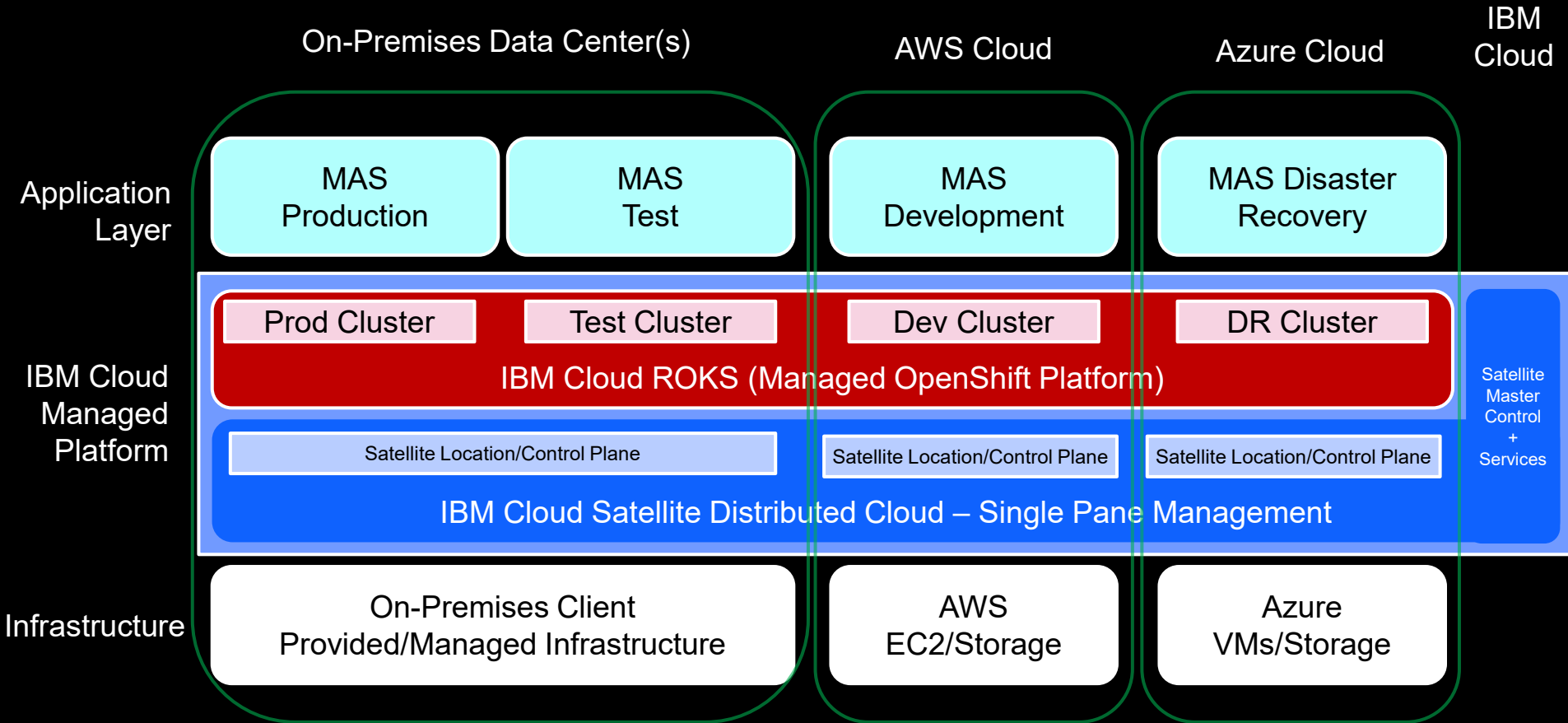
RHCOS = Red Hat Enterprise Linux CoreOS RHOCP = Red Hat OpenShift Container Platform

Consistent Architecture and tools across Hybrid multi-cloud and Edge locations



1. Consistent Developer and Operational experience
2. Fully Automated Deployments on other Clouds

Example MAS Hybrid and Multi-Cloud Management



SCC Workload Protection Runtime vulnerabilities reporting

The screenshot displays the SCC Workload Protection interface for Runtime vulnerabilities reporting. The left sidebar contains navigation options: Home, Insights, Vulnerabilities (selected), Posture, Policies, Network, Events, Investigate, and Integrations. The main content area shows a list of 100 scanned assets (out of 119 total). Each asset entry includes its path, a bar chart for 'In Use' status, a 'Vulnerabilities' bar chart, and a 'Policy Evaluation' status.

Asset	In Use	Vulnerabilities	Policy Evaluation
carlost-satellite > my-app > deployment/security-playground/security-playground docker.io/eyisdigitalr/security-playground latest	21 44 43	188 999+ 999+ 423 999+ 219	Failed
carlost-satellite > my-app > deployment/recommendationservice/server gcr.io/google-samples/microservices-demo/recommendationservice v0.3.8	5 21 21	15 247 350 17 398 32	Failed
carlost-satellite > my-app > deployment/loadgenerator/main gcr.io/google-samples/microservices-demo/loadgenerator v0.3.8	4 15 19	11 52 53 9 66 5	Failed
carlost-satellite > openshift/console > deployment/console > console quay.io/openshift-release-dev/ocp-v4.0-art-dev @ sha256:e67df1aec47e1dbxb139360d74655ff101aedbacf2c260e34182232bd11475a2	1 15 20	1 62 343 240 - 33	Failed
carlost-satellite > openshift/service-ca > deployment/service-ca > service-ca-controller quay.io/openshift-release-dev/ocp-v4.0-art-dev @ sha256:3387ecf963d3914706c949f41051f29057a2d66c93009e2a0f0fd50a4df1465	1 12 18	1 59 333 239 - 31	Failed
carlost-satellite > openshift/service-ca-operator > deployment/service-ca-operator > service-ca-operator quay.io/openshift-release-dev/ocp-v4.0-art-dev @ sha256:3387ecf963d3914706c949f41051f29057a2d66c93009e2a0f0fd50a4df1465	1 12 18	1 59 333 239 - 31	Failed
carlost-satellite > openshift/marketplace > pod/community-operators-gwqf > registry-server registry.redhat.io/redhat/community-operator-index v4.13	1 9 23	2 61 346 270 - 34	Failed
carlost-satellite > openshift/marketplace > pod/redhat-marketplace-mv42 > registry-server registry.redhat.io/redhat/redhat-marketplace-index v4.13	1 9 23	2 61 346 270 - 34	Failed
carlost-satellite > openshift/marketplace > pod/redhat-operators-c2f7 > registry-server registry.redhat.io/redhat/redhat-operator-index v4.13	1 9 23	2 61 346 270 - 34	Failed
carlost-satellite > openshift/marketplace > pod/certified-operators-27b2b > registry-server registry.redhat.io/redhat/certified-operator-index v4.13	1 8 21	3 61 346 270 - 34	Failed
carlost-satellite > openshift/marketplace > pod/certified-operators-mkg6 > registry-server registry.redhat.io/redhat/certified-operator-index v4.13	1 8 21	3 61 346 270 - 34	Failed

SCC Workload Protection Compliance posture management

The screenshot displays the SCC Workload Protection interface, divided into a main compliance overview and a detailed control view.

Compliance Overview (Left Panel):

- Section: **POSTURE Compliance > Results**
- Context: **my-app-zone** (CIS Red Hat OpenShift Containe...)
- Summary: 106 Requirements Evaluated, 55 Failing Requirements, 51 Passing Requirements
- Table of Requirements/Controls:

Result	Requirement / Control
✗	5.2.6 Minimize the admission of root containers
✗	5.2.5 Minimize the admission of containers with allowPrivilegeEscalation
✗	5.2.7 Minimize the admission of containers with the NET_RAW capability
✗	Container with NET_RAW capability
✗	1.2.4 Use https for kubelet connections
✗	1.2.12 Ensure that the admission control plugin ServiceAccount is set
✗	1.2.13 Ensure that the admission control plugin NamespaceLifecycle is set
✗	1.2.14 Ensure that the admission control plugin SecurityContextConstraint is set
✗	1.2.15 Ensure that the admission control plugin NodeRestriction is set
✗	1.2.20 Ensure that the --audit-log-path argument is set
✗	1.2.22 Ensure that the maximumRetainedFiles argument is set to 10 or as appropriate

[Load More...](#)

Control Detail View (Right Panel):

- Section: **CONTROL Container with NET_RAW capability**
- Severity: High
- Resource Count: +7
- Systemd: Sysdig
- Description: Assigns NET_RAW capability that allows binding to any address for transparent proxying any host address
- Context: CIS Red Hat OpenShift ... (1)
- RESOURCES OVERVIEW: 13 Evaluated (13 Failing, 0 Passing, 0 Accepted)
- RESOURCES EVALUATION: 13/13
- Buttons: Add Filter..., Download Report, Fail, Pass, Accept
- Table of Resources:

Workload/Type	Cluster	Namespace	Account ID	Labels
✗ loadgenerator View Remediation				
Deployment	carlost-satellite	my-app	-	2
✗ security-playground-security-playground				
Deployment	carlost-satellite	my-app	-	5
✗ redis-cart				
Deployment	carlost-satellite	my-app	-	2
✗ adservice				
Deployment	carlost-satellite	my-app	-	2
✗ emailservice				
Deployment	carlost-satellite	my-app	-	2
✗ paymentservice				
Deployment	carlost-satellite	my-app	-	2

SCC Workload Protection Events overview/summary

Workload Protection | Events Overview

Home | Insights | Vulnerabilities | Posture | Policies | Network | Events | Investigate | Integrations

Hosts: 3 Hosts of 3 (4 policies, 0 rules)

Kubernetes: 1 Clusters of 1 (2 policies, 51 rules)

Events By Severity: Bar chart showing 1 High event at Feb 8, 5:00:00 PM.

Top Policies:

Policy Name	Triggered
Sysdig Runtime Notable Events	29
Sysdig Runtime Threat Intelligence	1

Top Rules:

Rule Name	Triggered
Redirect STDOUT/STDIN to Network Connection in Container	28
Detect crypto miners using the Stratum protocol	1
Terminal shell in container	1

Events by MITRE ATT&CK® Tactic & Technique:

Tactic & Technique	Count
Reconnaissance (TA0043)	0
Resource Development (TA0042)	0
Initial Access (TA0001)	0
Execution (TA0002)	30
Persistence (TA0003)	0
Privilege Escalation (TA0004)	1
Defense Evasion (TA0005)	0
Credential Access (TA0006)	0
Discovery (TA0007)	0
Lateral Movement (TA0008)	0
Collection (TA0009)	0
Command and Control (TA0011)	1
Exfiltration (TA0010)	0
Impact (TA0040)	1
Command and Scri... (T1189)	28
Exploitation for Priv... (T1069)	1
Application Layer P... (T1071)	1
Resource Hijacking (T1496)	1

IBM