CAGS OpenShift for FREE project

Quality Assurance Review

10.05.2024

**Indice**

[***Introduzione 1***](#_heading=h.gjdgxs)

[***Progettazione e installazione Cluster ACM 2***](#_heading=h.30j0zll)

[***Modalità accesso ACM 2***](#_heading=h.1fob9te)

[***Network Policy 3***](#_heading=h.3znysh7)

[***Istio Policy e comunicazione con l’esterno 3***](#_heading=h.2et92p0)

[**Istio Policy 3**](#_heading=h.tyjcwt)

[**Comunicazione con l’esterno 4**](#_heading=h.3dy6vkm)

[***Regole di hardening 4***](#_heading=h.1t3h5sf)

[***Crittografia 5***](#_heading=h.4d34og8)

[***Observability 5***](#_heading=h.2s8eyo1)

[**Logging 5**](#_heading=h.17dp8vu)

[**Monitoring 6**](#_heading=h.3rdcrjn)

[**Tracing 6**](#_heading=h.26in1rg)

[***SentinelOne 6***](#_heading=h.lnxbz9)

[***Vault 7***](#_heading=h.35nkun2)

[***Disaster Recovery 7***](#_heading=h.1ksv4uv)

[**Quay 7**](#_heading=h.44sinio)

# Introduzione

CAGS ha richiesto in data 09.05.2024 ad NTT DATA, in quanto responsabile della quality assurance per il progetto FREE, di organizzare una serie di incontri interni allo scopo di verificare che quanto già progettato e in corso di implementazione per quanto riguarda i cluster Openshift in ambito FREE sia stato predisposto seguendo le best practice del vendor (Red Hat) e di progettazione architetturale, nonché i requisiti di sicurezza di CAGS.

I primi incontri sono stati tenuti in data 10.05.2024.

Presenti all’incontro sono:

* NTT DATA (Marano, Velotti, Cocuzzoli)
* Gruppo di Sicurezza
* Architetture CAGS
* Accenture
* Red Hat

Le tematiche sono state individuate tramite approfondimento sul DDS di Openshift, e incontri tenuti in precedenza con Red Hat e il gruppo di Sicurezza.

# Progettazione e installazione Cluster ACM

Dal DDS si evince progettazione di un doppio ACM, uno su Acilia e uno su Rozzano in configurazione attivo-standby, ognuno dei quali è agganciato a tutti i cluster presenti in tutti gli ambienti (sviluppo, collaudo, parallelo, produzione). Gli ACM saranno attestati su vlan di management, disgiunta da quella di produzione, che come da linee guida CAGS può raggiungere le console di tutti gli ambienti.

Per motivi di tempistiche è stato installato e testato un ACM sandbox temporaneo su parallelo. Tale installazione è tracciata anche nel DDS, come già richiesto da sicurezza.

Le installazioni in esercizio sono iniziate il 9 maggio.

**Stato: La predisposizione ACM è da best practice.**

**[RH] Si intende best practice CAGS?**

**Open point: nessuno.**

# Modalità accesso ACM

Nel DDS sono state descritte le modalità di accesso, solo gli admin lo possono raggiungere e solo tramite CyberArk.

Le utenze per ACM per accesso sono con gruppi AD di dominio.

Nel momento in cui ci si connette al link della console amministrativa, si accede tramite **gbcai**, si atterra su server ponte che veicola la sessione https verso le console, CyberArk si occupa di aprire la sessione sul server ponte e di inserire le utenze di gpcai.

**Stato: Su ACM sicurezza approva le modalità di accesso tramite CyberArk, il DDS risulta corretto su questo punto.**

**Open Point:**

* **Gaspare Sala: abbiamo sviluppato connettore cyberark per OCP, abbiamo testato, è stata mandata e-mail ai sistemisti (Giorgio Tarozzi) e l’integrazione è in mano a loro.**
  + **A me risulta che Bica/tarozzi hanno una mail per cui è chiesto di provare e dare un feedback, l’attività resta su sicurezza.**
* **C’è un tavolo gestito da sicurezza CAGS che fa test integrazione console di OCP sotto CyberArk, intanto sono state fatte aperture per permettere di raggiungere le console.**
* **A fine installazione sarà fornito a chi si occupa dell’integrazione anche il link degli ACM finali che ancora non sono stati installati, quelli forniti attualmente sono dei singoli cluster applicativi.** 
  + **Sono installati sono in corso operazioni di test DR**

# Network Policy **[RH] qui meglio parlare di network segregation per non confondere il titolo con le networkPolicy Kubernetes**

RH: sono stati discussi i flussi target da implementare per network segregation, ad oggi non è emersa la necessità di utilizzare authorization policy di Istio, da approfondire a parte.

[RH] come stabilito nella call del 10/5 e implementato in quella del 13/5, le policy di segregazione sono state implementate tramite le authorizationPolicy istio

Nel DDS sono descritte le aperture di rete e le regole infrastrutturali (excel allegato), e le regole applicative sono state inserite nei DDS di 3I e 3J.

Io terrei a riferimento la PPT sul microservizio che è chiaro e di fatto usato per

discutere aperture etc, facilita e molto la comprensione di quanto applicato.

Sicurezza conferma che quanto emerso su questo punto è conforme, la regolamentazione tra esterno/interno del cluster è stata predisposta come da best practice.

Sicurezza rimarca però che i POD possono spostarsi su qualsiasi worker, quindi con apertura verso tutta l’infrastruttura gestiamo in modo efficiente tutti gli accessi, ma c’è un tema aperto, la regola condivisa è che tutte le chiamate in ingresso e in uscita in https vengano veicolate dai micro-gw, se abilitiamo tutta la rete in https, non siamo sicuri che la chiamata esca esclusivamente dal micro-gw, se si potesse fare in modo che quando il micro-gw fa una chiamata in https uscente dal cluster, si presentasse con un IP o gruppo di IP, potremmo applicare una policy per cui saremmo sicuri che tutte le chiamate uscenti dal cluster passino dal micro-gw.

Da approfondire utilizzo degli Egress. **[RH] Il componente discusso è l'EgressIP**

**Stato: Seguite le best practice per la comunicazione interno/esterno.**

**Open point:**

* **Sicurezza chiede approfondimento su utilizzo micro-gateway**
* **Guglielmo chiede a Red Hat se si può usare un Egress solo per https o un determinato protocollo. RH dice che si dovrebbe poter fare ma va approfondito, RH esaminerà il requisito e invierà due-tre ipotesi di soluzione da discuter in call separata.**
* **La gestione delle policy richiede un processo di devsecops che non esiste in CAI, quindi attualmente sicurezza deve validare policy e devops la deve implementare. Incontro in programma tra ark/infra e sicurezza in merito alla gestione di questi temi, da monitorare l’evoluzione.** 
  + **Call fatta, prototipazione policy interna fatta e consegnata a Imola per implementazione pipe line**

**[RH] Il componente discusso è l'EgressIP**

# Istio Policy e comunicazione con l’esterno

## Istio Policy

Sicurezza ha rimarcato la necessità di Segregazione su base namespace, RH ha detto che solitamente in ambienti isolati e protetti non è indispensabile ma resta un requisito. Verrà quindi implementata tramite template Istio Policy che viene fornito da RH stessa.

**[RH] Come da minuta dell'incontro relativo: sono stati messi a disposizione degli esempi di policy da un repository esterno preparato per velocizzare e semplificare il test delle policy. Non si tratta tuttavia di un repository ufficiale Red Hat e quindi nè il contenuto del repository, nè i template risultanti da tali esempi sono oggetto di supporto"**

Nota importante. Non si può applicare la wildcard per i microgateway verso tutti i namepsace. Si deve gestire a livello di Authorization Policy in entrata al namespace di BE dell'applicativo. Quindi occorre settare tutti i namespace dei microgateway che possono comunicare verso un determinato namespace di BE.

Le policy vanno deployate sul cluster applicativo non su ACM.

MTLS è gestito dal service mesh che si occupa di gestire anche i certificati e la rotazione.

Sicurezza vuole sapere se esiste un tool grafico per la gestione delle policy, RH risponde che esiste solo una visualizzazione di come fluisce il traffico, non delle policy, utilizzando Kiali. Per le policy occorre usare gli yaml.

**[RH] È possibile consultare le policy e altre configurazioni, con anche alcune indicazioni circa il significato dei vari campi, tramite la sezione delle istio config di Kiali**

## Comunicazione con l’esterno

La comunicazione con l’esterno del cluster (egress) dev’essere regolamentata in modo da autorizzare solo determinati servizi (es. microgateway) a comunicare con sistemi esterni. Attualmente con quello che è stato già predisposto, dato che i pod di mgw sono deployati normalmente sui worker, occorre aprire tutta la rete dei worker tramite firewall per la comunicazione, il che consentirebbe a qualsiasi pod di parlare con l’esterno. Due soluzioni sono attualmente al vaglio:

Soluzione 1 **(molto impattante in termini di gestione)**: tramite service Entry. Si dice alla Mesh di consentire solo il traffico censito tramite Service Entry, e va censito tutto quello che è in uscita anche i database. Il cluster tratta le service entry come se fossero servizi interni, quindi bloccando la comunicazione interna viene impedita quella verso l’esterno.

Soluzione 2 **(Soluzione preferita dal GdL interno presente in call**) : mettiamo un egress per il microgateway con la 443 e lo facciamo andare in any verso l'esterno e un altro egress solo per quei casi che devono andare verso le farm WCF, visto che non possono passare dal microgateway.

Il dubbio di red Hat è che possa assumure un ip o un range di IP stabiliti oppure qualsiasi IP. RH farà un check offline e darà possibile soluzione per questa alternativa.

**[RH] Il componente discusso è l' EgressIP**

**[RH] Il componente EgressIP[1] permette di associare ai workload di un determinato namespace un range o una lista di IP in modo che poi il traffico esca con quell'IP sorgente, da un determinato set di nodi del cluster. Questa soluzione soddisfa il requisito di uscire con uno o più indirizzi IP pre-configurati, ma non gestisce la porta.**

**Un'altra possibilità è quella di utilizzare l'EgressFirewall[2] questo componente funziona sostanzialmente come una network policy di tipo egress (la differenza è che deve essere gestita a livello di cluster e che gestisce il solo traffico in uscita dal cluster), in questo modo è possibile specificare filtri sul traffico in uscita dai namespace, anche specificando porta/protocollo**

**Un'ulteriore possibilità è quella di combinare le attuali istio AuthorizationPolicy con delle network policy di tipo egress, dove appunto specificare i filtri da applicare al traffico in uscita dai vari namespace.**

**Nell'opzione EgressFirewall e Network Policy è necessario verificare l'applicabilità delle soluzione considerando anche:**

* **Requisiti target di filtro/segregazione del traffico in uscita dai namespace e dal cluster**
* **Attuale configurazione delle AuthorizationPolicy Istio per il traffico intra-cluster**

**[1]**[**https://docs.openshift.com/container-platform/4.14/networking/ovn\_kubernetes\_network\_provider/configuring-egress-ips-ovn.html**](https://docs.openshift.com/container-platform/4.14/networking/ovn_kubernetes_network_provider/configuring-egress-ips-ovn.html)

**[2]**[**https://docs.openshift.com/container-platform/4.14/networking/ovn\_kubernetes\_network\_provider/configuring-egress-firewall-ovn.html**](https://docs.openshift.com/container-platform/4.14/networking/ovn_kubernetes_network_provider/configuring-egress-firewall-ovn.html)

**Stato:**

* **Istio policy, l’idea attuale segue le best practice di sicurezza CAGS, vanno implementate -> Fatto**
* **Non possibile usare tool grafici per le policy, implementabili tramite yaml**
* **Non implementate attualmente soluzioni definitive per gestione traffico Egress.**

**Open Point:**

* **Implementare policy Istio -> Fatto**
* **Trovare soluzione per [RH] traffico Egress, due al vaglio (di cui la seconda preferita dal GdL interno presente in call), attesa proposta RH**
* **Aggiungerei però che sicurezza ha avallato il controllo tramite (ipotizzato egrees) per la 443 dai microgateway, dato che è stata aperta in uscita verso qualsiasi ip del proprio ambiente. La gestione delle aperture differenti (es DB.. .o altro) seguono l’iter standard di apertura lato firewall (migliorabile) ma al momento questo basta. (Tra l’altro riportato nel DDS)**

**[RH] Visto che si tratta di un documento chiamerei le istio policy con il loro nome puntuale: istio AuthorizationPolicy**

# Regole di hardening

Sicurezza vorrebbe un documento relativo alle regole di hardening. -> è attività di sicurezza.

RH specifica che ci sono strumenti a bordo del cluster che permettono di applicare profili di sicurezza che seguono standard di mercato. Diverse cose lato sicurezza che prima erano applicate sui nodi di mirantis non saranno necessarie perché i nodi di openshift usano coreos che è una versione con una superficie di attacco ridotta rispetto ad altre distribuzioni linux, per cui non necessita di hardening particolare, ma si possono applicare misure aggiuntive.

**Stato: da verificare le best practice utilizzando documentazione hardening openshift fornita da RH che dev’essere confrontata con manuale hardening CAGS fornita da sicurezza, con output analisi di gap tra i due. Allo scopo va istituito tavolo dedicato tra Sicurezza, RedHat e NTT DATA.**

**Open Point:**

* **Hardening OCP standard vs Hardening CAGS**
* **Scrittura manuale di Hardening CAGS per OCP**

# **[RH] Qui trovate alcuni spunti per gli aspetti da valutare per l'hardening di OpenShift[1] e qui alcune considerazioni su come si possono applicare le modifiche ai nodi CoreOS (visto che come detto già in call si tratta di un sistema operativo già immutabile)[2]**

# **Un buon esempio da cui partire è lo standard CIS, dal sito di CIS è possibile scaricare l'ultimo benchmark per le varie distribuzioni Kubernetes, tra cui OpenShift[3]**

**Il compliance operator[4], citato anche nella call, è uno strumento installabile sul cluster OpenShift per confrontare lo stato del cluster con uno o più benchmark standard (come CIS) o customizzati. Da questo punto di vista può essere un elementi in più per tenere sotto controllo la security posture del cluster ed è possibile anche monitorare l'esito di questi controlli tramite policy ACM[5]**

**[1]**[**https://docs.openshift.com/container-platform/4.14/security/?extIdCarryOver=true&sc\_cid=701f2000001Css5AAC**](https://docs.openshift.com/container-platform/4.14/security/?extIdCarryOver=true&sc_cid=701f2000001Css5AAC)

**[2]**[**https://docs.openshift.com/container-platform/4.14/security/container\_security/security-hardening.html**](https://docs.openshift.com/container-platform/4.14/security/container_security/security-hardening.html)

**[3]**[**https://www.cisecurity.org/benchmark/kubernetes**](https://www.cisecurity.org/benchmark/kubernetes)

**[4]**[**https://access.redhat.com/documentation/en-us/openshift\_container\_platform/4.14/html/security\_and\_compliance/compliance-operator**](https://access.redhat.com/documentation/en-us/openshift_container_platform/4.14/html/security_and_compliance/compliance-operator)

**[5]**[**https://access.redhat.com/documentation/en-us/red\_hat\_advanced\_cluster\_management\_for\_kubernetes/2.5/html/governance/governance#ocp-cis-policy**](https://access.redhat.com/documentation/en-us/red_hat_advanced_cluster_management_for_kubernetes/2.5/html/governance/governance#ocp-cis-policy)

# 

# Crittografia

Crittografare dati a riposo e in transito.

Sicurezza ribadisce che il traffico deve essere cifrato anche all’interno del cluster.

Secondo Infra CAGS, Per la crittografia “at rest” lato infra è stata dedicata una persona direttamente da Ottolini, ad oggi non risulta che sia richiesta.

Tuttavia la richiesta è insita perché viene dalla normativa quindi è vincolante.

Su questa tematica è necessario un punto fermo dal PMO o chi decide:

1. Crypto flussi è già un prerequisito noto e adottato da CISO

2. Crittografia o altro derivante da DORA non mi risultava dovesse impattare il

progetto proprio perché appena partita analisi interna sull’argomento con stream

dedicato (farei chiarezza una volta per tutte su questo punto).

**Stato: Attualmente nel DDS non è presente nessuna soluzione per la crittografia at rest.**

**Open point:**

* **Trovare soluzione per crittografia at rest -> O mi è sfuggita o non ho ingaggi formali sul tema. (Vedi sopra)**
* **Non vincolante per andare in produzione ma tema da affrontare -> nel progetto free? Io chiederei ingaggio formale dal PMO (se necessaria)**

# Observability

## Logging

Nel DDS è presente una trattazione del logging audit, e del Siem.

Nel DDS c’è la parte del forward di vector, lasciata ad alto livello perché lato CAGS siamo in attesa di metriche di sicurezza. Vector è stato installato ma va configurato.

Non è ancora stato predisposto né Garante 1 (accesso amministrativo) né Garante 2, che sarà una soluzione applicativa, al Siem è gradito inviare anche informazioni per implementare controlli di sicurezza.

I log applicativi al momento sono tutti dentro loki, è stato aperto uno stream con Reply, perché esiste il tema dell’aggregato da riportare su splunk.

Va verificata la versione di Loki disponibile.

Per l’accesso ai log tramite la console di Openshift è stato predisposto per la collaudo e parallelo (e sarà uguale in produzione) un gruppo AD full read in cui si ha accesso in sola lettura ai componenti del cluster in sola lettura (esclusi i secret) segmentati per RGP, in modo che ognuno possa accedere solo ai log dei namespace consentiti. Viene usato il ruolo “openshift-viewer-loki”.

È il modello già usato per mirantis e per tutti i cluster kubernetes.

La retention è come da indicazioni di Zuppa.

## Monitoring

Per le metriche infrastrutturali ACN sta portando avanti webhook per integrazione con alerta, dynatrace è in corso di configurazione (acquisto licenze).

Per le metriche Infrastrutturali si utilizza un tool proprietario di openshift , Thanos (versione RH di Prometheus) che manda gli alert direttamente su Alerta. Va descritta la soluzione su DDS o come allegato allo stesso.

**[RH] OpenShift non ha alcun tool proprietario, ma solo componenti Open Source. Thanos (**[**https://thanos.io/**](https://thanos.io/)**) è una tecnologia completamente differente rispetto a Prometheus (**[**https://prometheus.io/**](https://prometheus.io/)**). Per le metriche, OpenShift utilizza Prometheus all'interno dello stack incluso in OpenShift Monitoring.**

## Tracing

Su produzione si userà Dynatrace

Jaeger viene installato con operator di service mesh, attualmente su collaudo non si vede perché service mesh non è stato configurato, fa parte delle configurazioni di istio (ortogonale al tema istio policy).

Ho fatto un approfondimento e “Jaeger” sarà “discontinuato” dalla 4.14 (nostra versione) in

favore di “tempo”:

[Installing - Distributed tracing | Observability | OpenShift Container Platform 4.14](https://docs.openshift.com/container-platform/4.14/observability/distr_tracing/distr_tracing_jaeger/distr-tracing-jaeger-installing.html)

Per

[Installing - Distributed tracing | Observability | OpenShift Container Platform 4.14](https://docs.openshift.com/container-platform/4.14/observability/distr_tracing/distr_tracing_tempo/distr-tracing-tempo-installing.html)

Ora, installare un prodotto a breve abbandonato non mi pare il caso, se installiamo Tempo

andrebbe capito se poi si sa usare.

Per parallelo/produzione facciamo tracing con dynatrace

Per sviluppo/collaudo attualmente si è configurato tracing con jaeger.

**Stato: da integrare il DDS, debito tecnico sia su logging, sia su monitoring che su tracing**

**Open Point:**

* **inoltro dei log infrastrurrali al SIEM non è stato realizzato. Va previsto -> Individuare referente per l’attività e schedularla. Temi indirizzati da sicurezza?**
* **C'è vector installato ma non c'è il forward dei log di Garante 1, e i log del SIEM. Gap da colmare. -> ideam C.s.**
* **log garante 2 sarà soluzione applicativa, al siem è gradito inviare anche informazioni per implementare controlli di sicurezza. Infrastruttura + Sicurezza dovranno configurarlo insieme -> ideam C.s.**
* **Per sviluppo/collaudo facciamo tracing con jaeger (debito tecnico) -> Attenzione quanto riportato sopra.**
* **Da capire se in attesa di dynatrace conviene inserire jaeger anche per parallelo -> Lo valuterei post collaudo ma tendenzialmente non sono d’accordo, sono comunque soluzioni che impattano il cluster.**
* **Acquisto licenze dynatrace in corso -> Attenzione potremmo andare oltre tempi di progetto**
* **Inserire soluzione di Monitoring completa su DDS o come allegato. -> perché questo punto? Non avevamo detto che cade in monitoraggio standard già indirizzato e contrattualizzato su ACN?**

**Possiamo aggiungere nota:**

**Per non modificare le modalità di monitoraggio standard definite con CAI si procederà ad inviare gli allert del cluster Openshift verso il sistema Alerta del Command Center ACN – attraverso webhook.**

**Nota:**

**Per integrazione con il sistema Alerta del command Center ACN è necessario configurare su ironport https://alerta.it.accenture.com/**

# SentinelOne

**Stato:**

**In collaudo è installato, in parallelo è installato su acilia, e su rozzano è in corso l’installazione (c’è una issue che dovrebbe essere stata indirizzata con un ticket al vendor). -> Rozzano ok**

**Open point:**

**stato della configurazione all’interno di Sentinel. Si deve lavorare su namespace a differenza si mirantis dove c’è configurazione per macchina, c’è stato approfondimento col vendor e si può fare, è solo una questione di implementazione, da chiedere a Antonio Di Domenico avanzamento dell’attività.**

# Vault

Per quanto riguarda Vault o alternative (es. Conjur), Gaspare Sala ha ribadito che è in partenza congiuntamente al gruppo di Architetture una POC per valutare le varie soluzioni, c’è un kick-off in questa settimana, ma dato lo stato siamo ancora lontani ad avere in produzione una soluzione per la gestione dei secret e al momento non abbiamo una data target.

I secret attualmente sono presumibilmente gestiti localmente.

Sicurezza attualmente detiene le password salvate sul vault di cyberark. Ad oggi non c’è interazione diretta, cyberark viene utilizzato come repo delle password. Vengono usati secret di tipo registry standard e c’è un operatore che li inserisce manualmente.

**Stato:**

* **Il processo attuale di gestione secret è quello standard.**
* **I secret sono solo codificati in base64, c’è un profilo in sola lettura per evitare che persone non autorizzate possano aprire i secret.**

**Open Point:**

* **POC per valutare diverse soluzioni di gestione secret**

# Disaster Recovery

Per quanto riguarda eventuali failure di storage e connettività, restano al di fuori del DDS di OCP, perché fa parte di infrastruttura generale, c’è un documento ad hoc in CAGS che regola quelle casistiche (LLD).

Il DR dell’ACM prevede invece uno switch del Cluster attraverso attivazione o disattivazione del cluster in stand by verso Datacenter secondario e switch S3 in configurazione Mirror. Viene switchato il puntamento con pool di IP sull’F5. (questo è vero

per le parti applicative ospitate dal cluster OCP. Lo switch viene effettuato intervenendo sui

pool di F5). Per ACM hai semplicemente due console differenti tra ACILIA e ROZZANO.

[RH] Il DR dell’ACM prevede 2 istanze di ACM in configurazione active-standby con replica dei dati. In caso di fault dell’istanza active, è sufficiente modificare una variabile, sulla configurazione lato restore, in modo tale che l’istanza standby carichi le configurazioni e prenda il controllo dei cluster precedentemente gestiti dall’istanza active.

Per quanto riguarda OCP, invece, dato che il cliente ha dichiarato che i workload sono tutti stateless, si è optato per avere 2 cluster sempre attivi (acilia e rozzano) su cui verranno fatti sempre in simultanea i deploy dei workload ed in caso di fault verranno cambiati i puntamenti lato F5.

Per quanto riguarda il DR di Quay.

In accordo con il cliente Accenture dichiara che:

1. In ambiente di parallelo esiste una sola istanza di quay ad Acilia.

2. In produzione sono previste due istanze indipendenti di Quay (acilia/rozzano) non è previsto DR perché le immagini saranno deployate su entrambi i registry

**Stato:**

* **DDS prevede DR su ACM**
* **DR infra e connettività sono previsti in generale su documentazione CAGS**
* **Non si rilevano criticità in tema**

**Open Point:**

* **DR Quay (io non lo considero un openpoint, faremo un passaggio con DevOps quando ci arrivano ad utilizzarlo almeno dal collaudo)**

## Quay

Per l’ image scanning, è stata rispettata la politica CAI, è attiva per quay solo in collaudo ma non per ambienti superiori.

Viene realizzato con questa logica perché le modifiche vengono fatte solo su collaudo, poi la promozione avviene solo tramite pipeline, per questo non sono state introdotte le scansioni su ambienti superiori, anche perchè image scanning è cpu intensive.

**[RH] La scelta di disattivare lo scan per le immagini su alcuni ambienti non è scelta indicata da Red Hat, ma una scelta puramente dettata da considerazioni del resto del gruppo di lavoro su resource saving e non dettata da considerazioni di carattere tecnico. Sicuramente lo scanning richiede risorse che si vorrebbero risparmiare per altro, ma questo non implica che la funzionalità abbia consumi anomali**

**Stato:**

* **Tematiche riportate nei DDS, è da best practice**

**Open point:**

* **~~DR e failover, vedi sopra~~**