Minute CDG 18/02/2022

Introduzione:
CDG basato su Migrazione ai Token
Quindi non ci sono i reparti Rete e Infrastruttura presenti. Inoltre, non ci sono interventi significativi in programma.
Presenti solo i reparti Farm e Storage: stato + passaggio ai token (dismissione gridftp – abbandono globus).

Le milestone di wlcg si stanno avvicinando.
Per es: entro marzo 2022 tutti i servizi storage dovranno dare supporto token.

Richiesto anche agli esperimenti lo stato sui token.

Farm -> Slide
Utilizzo simile all'ultimo mese
Nuove Risorse (schede mellanox a fine giugno) => prima di luglio non sarà possibile installarle (down necessario)

Lo storage del vecchio sistema di virtualizzazione ha iniziato a rompersi dopo 5 anni, appena è stato messo fuori assistenza

Nuova gara -> info su slide.
Grossa incognita sui tempi di consegna

Stato di Linux: CentOS8 EOL 2021 – stiamo usando 8stream (versione più instabile).
CentOS 9 stream da dicembre.
CentOS 7 supporto fino a metà del 2024.

HTCondor: Accounting e monitoring LHC.
Alice sta usando solo job multicore. Conseguente calo di job running di CMS, mentre LHCb ne ha giovato perché usa single-core.
Atlas rimane leggermente sotto-pledge
DanieleSp: cos'è la linea rossa? Job pending

TOKEN Roadmap e stato.
Problemi aperti.

DanieleC: questa parte è stata discussa su auth wlcg?

SDP: ieri c'è stata una riunione: si è parlato del token renewal senza conclusioni – Ale Forti osservava che al tempo di quando si metteva su GSI c'era la stessa discussione per i proxy – quindi ci sono le stesse discussioni di anni fa.
Rinnovare i token non sembra così semplice..

FracnescoG: token renewal – funziona bene con IAM – però c'è il timore che se IAM va giù, i token non rimangano validi, per esempio per un we. Inoltre, un token che viene utilizzato per sottomettere un job non serve più – è importante capire che in teoria ogni token ammette un'operazione specifica – uno per sottomissione, uno per data management (questa è la teoria – da capire ancora la pratica).
Il subject inoltre rimane così - UUID (sequenza casuale di lettere e numeri – non prevedibile).
Condor deve accettare dei token in cui ci sono i gruppi (per es) e fare callout ad argus.

SDP: ok, sulle operazioni specifiche, ma rimane da capire come il job ottiene token per le altre operazioni. Va bene mappare subject distinti su unico username – con condor si può avere stesso utente Unix che lavora con differenti accounting group e quindi diversi fairshare.

Spardi: questa limitazione è di condor-CE. A partire dalla versione 3.6, ci sarà questa problematica ufficialmente su tutti i siti anche non OSG?

DanieleSp: per l'Europa, quando va fuori vita condor che supporta proxy per settembre/ottobre – può darsi che ci sia uno shift perché gli exp sono un po' indietro. Non lo farà neanche OSG adesso.

SilvioP: condor vuole che utenti siano mappati staticamente.

DSP: Il processo di migrazione è più lungo di quel che sembra. Per esempio, anche xrootd non è pronto.

FrancescoG: una cosa è la dipendenza da globus e una cosa è supportare x509 – da capire bene.

MatteoDur: AMS, Dampe, Herd – job locali rimangono così? Senza auttenticazione?
Spazio AMS accessibile via XrootD con voms-proxy, non sarà così? È corretto?
I token in tal caso chi me li darà? Con tecnologia tipo IAM?

DanieleC: Stiamo guardando le timeline di wlcg.
Un po' di flessibilità per i no-LHC, però accadrà anche per loro.
Sottomissione locale non cambia.
IAM al posto di VOMS – exp per exp sarà gestito caso per caso. La transizione comunque dovrà avvenire.
AMS vivrà altri 6 e 7 anni, per cui subirà anch'esso la transizione. Sottomissione a mano rimane.

SDP: i job di AMS sottomettono locale con certificato – solo alcuni.
Causa aggiornamenti la flessibilità non è tanta.

Alice -> Slide

SDP: Alice solo multicore?
FN: ci stiamo muovendo su multicore perché run3 richiede solo quelli. A Run3 sarà proprio così.
Adesso che siamo in perdiodo di transizione è misto, la sottomissione è mista.

Storage -> Slide

FrancescoNof: Aumentare a 1.6PB per Ceph non dovrebbe essere un problem.

VS: Problema di un solo redirector significa non ridondanza.

DanieleSp: sia l'alias che redirector dati all'utente? Sì.
Il redirettore dava timeout error, per cui è stato cambito con un endpoint fisso, ma cambiati i server non funzionava più. L'alias adesso non gli funziona e non sappiamo perché. Quindi stanno usando adesso il redirettore interno, ma stanotte hanno ottenuto un "permission denied" su un file. Da capire il problema.

DanieleSp Indaga inoltre internamente per la fix di Rucio e per una directory su buffer che non migra.

SPer: LHCb fa sapere per passare su http per tape – però sembra che già sia utilizzato.

ATLAS -> slide
LRin: Sarebbe curioso cosa fanno i job di Atlas su ce07 e che meccanismo utilizzano per scrivere sullo storage. Capire se poi usa ancora i token per fare DM, ma credo sia ancora utilizzato x509.

FG: sembra che Panda faccia arrivare al pilot anche il voms-proxy (no token) quindi sembra così, che usi x509 per fare DM dentro al Job.
SDP: conferma quanto detto da FG. C'era stato scambio di mail con Vokac – token solo per auth al CE – in particolare il token non viene trasferito al job in Condor.

DanieleC: torna con il fatto che ogni token è usato per operazioni specifiche.

FG: in questo modello, al posto del proxy si può far arrivare un token. Tecnicamente sembra fattibile.

FG: IAM server è pensato per essere unico per ogni VO. Per ogni operazione chiedere un token e inoltre IAM è unico: ce ne è uno solo. L'unica cosa è che si può fare è metterlo in HA. Distribuire IAM geograficamente non è mai stato pensato, di metterlo in HA certo, ma è comunque sempre UNICO. Anche legalmente non sembra una cosa facile da applicare.

DanieleSp: indip dall'HA. Se è in produzione il servizio deve essere in HA. Avere l'HA è un problema del sito o dell'esperimento?
FG: del sito.
FedericaAgo: lo stato è in fase di test. IAM vero con un cluster di Test.
FG: supponendo che funzioni, ci vuole una release di IAM. E poi l'ostacolo della controparte al cern per il deployment – al momento al cern non c'è nessuno che si occupa di queste cose.
DanieleSp: passiamo ai token, ma IAM è preliminare a tutto.
FG: sì, atlas fa così. IAM funziona – non è bloccante.

SDP: è possibile che il master attivo sia uno solo, ma quando va giù la replica prende tutto lo stato del master fino all'ultima azione non commitata? Anche se distribuita geograficamente.
FG: immagino di sì, qui però non è mai stato applicato. Però se per esempio va giù il collegamento al CERN sarebbe un problema anche se ridondato. Ci sono altri tipi di problemi.

SilvioP: nel wg di auth wlcg si è proposto l'utilizzo degli SCI-token. Non ho capito la differenza. Anche questo sistema ha un singolo registro. Voi sapete qualcosa in più rispetto a IAM?
FG: Non conosco SCI-tokens – mi sembra che in questo caso ci possono essere più issuer distribuiti di token per i pilot, però si rimane su IAM.

FG: Anche vedere la scala di richieste al secondo sarebbe interessante da analizzare.

CMS -> Slide

SDP: dsicrepanza dei pledge. Serve un po' di tempo per guardarci. Organizziamo call di una o due ore.
DanieleSp: sentiamoci offline.

LHCb -> Slide

DanieleC: uno scosatemento pledge CPU verso il basso ce lo aspettiamo. Mentre per CMS va capito.

DSp: Sì, dovremmo capire la discordanza tra le metriche, non il motivo per il sottopledge per CMS.

Belle II -> Slide

Cristina e Silvio si sentono la prossima settimana per ultimare la configurazione di IAM – integrato con VOMS.

NO – LHC -> slide

DanieleC: area tape Neutrino – "capire cosa intendono con accesso da user interface".
DanieleC: non abbiamo citato virgo xperché non ci sono stati problemi.
LRei: volevo citare i token. Virgo non ha preso una posizione sui token. Interessato a provarli.
DanieleC: uno IAM è già disponibile per virgo.

Virgo

Bagnasco: dovremmo riprendere le discussioni. Problemi su come vorremmo che ligo trattasse le nostre identità, dopodiché riprendiamo il discorso token.