ATLAS Storage

- SE tokens deployment status & tests ... ~ ⅔ done

Resource	# SE X.509	# SE old token	# SE new token	# RSE enabled
DATADISK[davs]	60	43 (72%)	40 (67%)	30 (50%)
DATADISK[xroots]	50	33 (67%)	30 (60%)	0
SCRATCHDISK[davs]	59	42 (71%)	39 (66%)	35 (58%)
SCRATCHDISK[xroots]	48	32 (67%)	29 (60%)	0

- New ATLAS IAM token issuer https://atlas-auth.cern.ch/ (reasons, GGUS)
- Still no ATLAS SAM probes to test storage
  - SE token deployment validation done with our custom tests
    - Quick hack to be able to move forward with deployment (compliance tests: 1, 2, 3)
  - Plan to create SAM probes based on CMS code ADCINFR-272
- Not yet started to work on user interaction with tokens
  - Not clear why sufficient functionality can't be integrated directly in IAM

some compliance issues in all SE implementations

ATLAS CE and WFMS

- CE job submission with token (easy)
  - Solved issue for HTCondor-CE, used in production
  - ARC-CE sites not yet pushed to tokens for job submission (X.509 still works)
- Initial support for tokens in WFMS (Panda & pilot)
  - Panda and pilot rely exclusively on WLCG JWT tokens
  - For some use-cases long-lived access tokens necessary
    - Currently not allowed by WLCG JWT profile
      - Out of scope for EGI recommendations (WLCG use-cases are special)
    - Idea to extend WLCG JWT profile with special scope(s)
      - Allow long lived access token but with "risk analysis"
      - RP should normally reject access tokens with lifetime > 6h
  - Tokens currently used only internally / not used by end users
- Resouces managed by Harvester vs. aCT+ARC-CE with data management
  - ARC-CE data management useful for special resources (HPC)
  - Increased complexity in ARC-CE to support transfers with tokens
    - Started internal discussion how to move forward with tokens in this area

Traditionally pilot transfers data, ARC-CE with DM duplicate this functionality and needs transfer tokens

IAM service performance and availability

- Designing secure application with tokens
  - Different requirements and consequences
    - Single powerful X.509 VOMS proxy sufficient for everything on grid
    - 4 days long proxy could cover relatively long issues with VOMS service
  - Tokens comes with higher granularity
    - IAM token issuer downtime – almost instant failures or stuck jobs waiting for AT
  - Token issuer reliable otherwise "500k core becomes idle in an hour"
    - "Weekend without grid" will likely cause significant dissatisfaction among many stakeholders
    - T0 affected indirectly (raw data not cleared from P1 buffer till declared in Rucio)
- Token rates
  - File specific access tokens (only) for deletions – in average ~ 50Hz (~ 4M files daily)
    - Should be increased by ~ 30% to cover transfer failures (deletion of partially transferred file)
  - Not yet estimated for jobs (1M jobs transfers 5M files every day in ~ 250 PQ at 160 sites)
    - If we can avoid file specific tokens than number of tokens scale roughly with number of sites
  - It would be nice to have order of magnitude higher performance to cover all peaks