



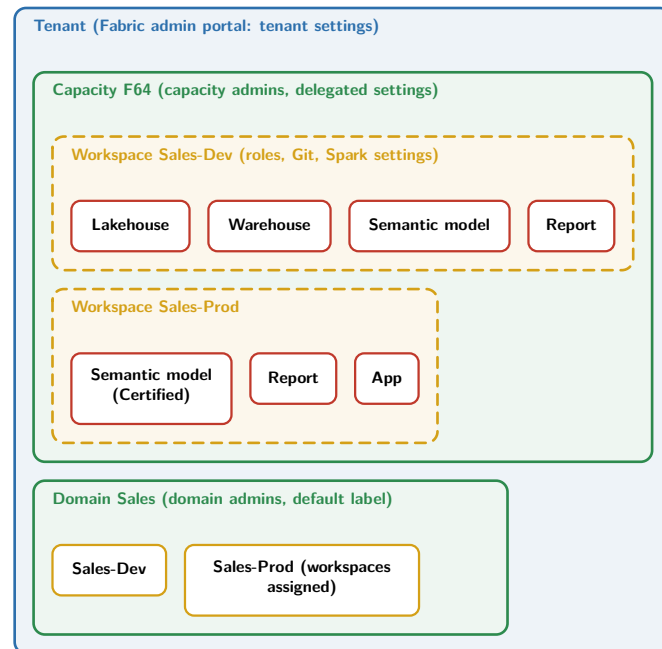
DP-600 Maintain (1): Capacity, Security and Governance

Microsoft Learn DP-600 skills outline and Microsoft Fabric documentation, as of 2026 | Tenant, capacity, domain, workspace and item hierarchy, F SKUs, smoothing and throttling, workspace roles, item permissions, OneLake security, RLS/CLS/OLS, dynamic data masking, sensitivity labels, endorsement, auditing

DP-600 Maintain Security Governance Capacity

Hierarchy and capacity

Where settings and permissions live



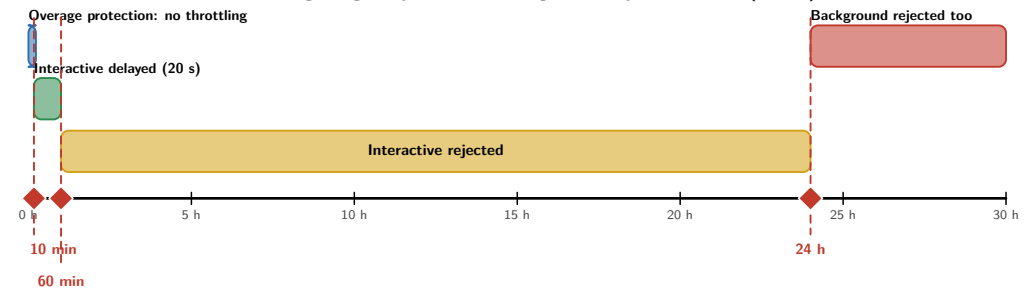
Topic	What to know
SKUs	F2, F4, F8, F16, F32, F64, F128 ... F2048; F64 ≈ former Power BI Premium P1
Licences for viewers	on F64 and above, users with a free licence can view Power BI content; below F64 each viewer needs Pro or PPU; authors always need Pro or PPU
Billing	pay-as-you-go per second (pause to stop compute billing; OneLake storage billed separately) or a 1-year reservation; scale up/down in the Azure portal

Capacity Metrics app per-item CU usage, smoothing, overages, throttling; the first stop for 'reports are slow at 10 am'

Spark Spark jobs consume capacity CUs (1 CU = 2 Spark vCores); burst factor up to 3× for Spark; Autoscale Billing for Spark can move Spark to pay-as-you-go

Surge protection capacity setting that rejects background jobs above a threshold to protect interactive use

Throttling stages by future overage already consumed (hours)



How much of an F64 a nightly job really uses

FORMULA $U = W / (C \times T)$

WHERE

- U = average share of the capacity used over the smoothing window (0-1)
- W = work of the operation, from the Capacity Metrics app (CU-seconds)
- C = capacity units of the SKU (F64 = 64) (CU)
- T = smoothing window: 86,400 s for background, ≥ 300 s for interactive (s)

WORKED

W = 2880000
C = 64
T = 86400
 $U = 2\,880\,000 / (64 \times 86\,400)$
U = 0.5208

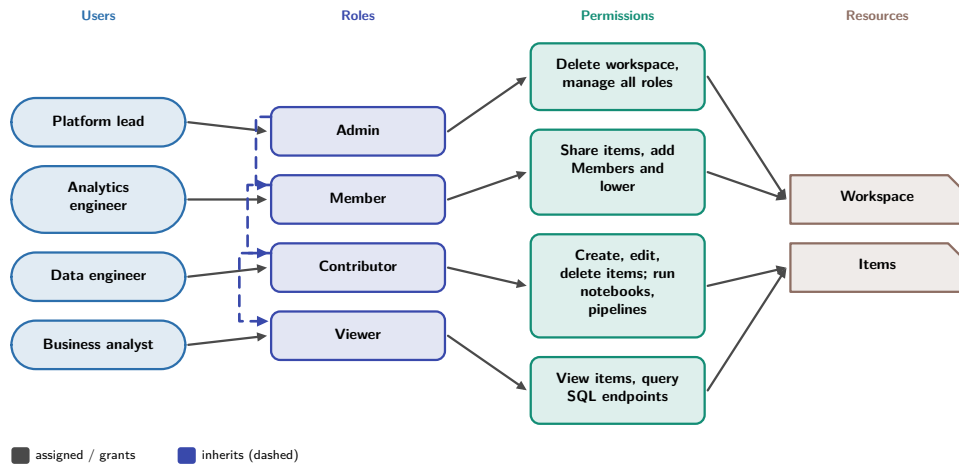
RESULT U = 0.5208

READ IT 0.52: the background refresh occupies 52 % of the F64 around the clock for 24 hours, leaving 48 % for interactive report queries; add more such jobs and interactive queries start being delayed.

MISTAKES

- Reading the job's peak instead of its smoothed share
- Forgetting that pausing the capacity settles the remaining smoothed usage as a charge
- Treating Spark vCores as CUs (1 CU = 2 Spark vCores)

Workspace roles and item permissions



Need	Grant	Why not more
Analyst builds own reports on a certified model, no workspace access	item share: Read + Build on the semantic model	Viewer role exposes every item of the workspace
Data scientist reads lakehouse files with Spark from another workspace	item permission ReadAll (or OneLake security role)	Contributor can also delete items
SQL user queries the warehouse only	item share Read + ReadData, then GRANT/DENY in T-SQL	workspace roles bypass object-level GRANTS
Report consumers in Prod	workspace app audience or Viewer	Contributors are not filtered by RLS
Admin of the platform settings for a business unit	domain admin or capacity admin	Fabric administrator is tenant-wide

⚠ RLS does not filter workspace editors

Semantic-model row-level security applies to users with **Viewer** role or item Read permission only. Admins, Members and Contributors of the workspace see all rows. Test roles with 'View as' in the service or Desktop; publish consumers through an app or Viewer role.

🔒 Data-level security in each engine

Warehouse / SQL analytics endpoint: CLS, RLS, masking (T-SQL)

```
GRANT SELECT ON dbo.Customers (CustomerId, Name, Region) TO [analysts];
DENY SELECT ON dbo.Salaries TO [analysts]; -- object level
CREATE FUNCTION sec.fn_region(@Region varchar(20))
RETURNS TABLE WITH SCHEMABINDING AS
RETURN SELECT 1 AS ok FROM sec.UserRegion u
WHERE u.Region = @Region AND u.Upn = USER_NAME();
CREATE SECURITY POLICY sec.RegionFilter
ADD FILTER PREDICATE sec.fn_region(Region) ON dbo.Sales
WITH (STATE = ON);
ALTER TABLE dbo.Customers ALTER COLUMN Email
ADD MASKED WITH (FUNCTION = 'email()');
GRANT UNMASK TO [support-leads];
```

Semantic model: dynamic RLS role (DAX table filter on DimSalesRep)

```
-- role "Reps", table DimSalesRep, filter expression:
[Email] = USERPRINCIPALNAME()
-- managers see their team (security table with a path column):
PATHCONTAINS ( DimSalesRep[ManagerPath],
LOOKUPVALUE ( DimSalesRep[RepId],
DimSalesRep[Email], USERPRINCIPALNAME () ) )
```

Control	Warehouse / SQL endpoint	Semantic model	OneLake (lakehouse)
Rows	security policy (RLS)	RLS roles (DAX), dynamic with USERPRINCIPALNAME()	OneLake security row rules (check GA status)
Columns	column GRANT / DENY (CLS)	OLS (Tabular Editor / TMDL)	OneLake security column rules
Objects	GRANT/DENY on tables, views, schemas	OLS on tables	data access roles on tables/folders
Masking	dynamic data masking + UN-MASK	-	-
Files	-	-	data access roles on Files folders

- **Direct Lake caveat** a Direct Lake on SQL endpoint model that reads a table protected by SQL RLS/CLS falls back to DirectQuery so the SQL rules apply; define security in the model or in OneLake security instead
- **Sensitivity labels** applied manually, by default label policy or inherited from sources; flow downstream (lakehouse → model → report) and protect exports to Excel, PowerPoint and PDF; mandatory labelling is a tenant setting
- **Endorsement** Promoted by any item owner with write access; Certified only by users the Fabric admin authorises; Master data for authoritative reference items; endorsed items rank first in the OneLake catalog
- **Audit and monitoring** Fabric activities land in the Microsoft Purview audit log; workspace monitoring writes item logs to an eventhouse; the admin monitoring workspace gives tenant usage reports

🚩
 Recap and self-test

Statement	True	False
1. Viewers with a free licence can open reports in a workspace on an F32 capacity → Free viewing needs F64 or larger; below that viewers need Pro or PPU.	☐	☒
2. A Contributor can share an item with another user → Sharing and managing access needs Member or Admin (or Reshare permission on the item).	☐	☒
3. Background operations are smoothed over 24 hours → Interactive ones over at least 5 minutes.	☒	☐
4. Semantic-model RLS filters workspace Members → Only Viewers and users with item Read are filtered.	☐	☒
5. Build permission lets a user create new reports on a semantic model → Combined with Read; no workspace role needed.	☒	☐
6. Certified endorsement can be applied by any workspace Admin → Only users or groups the Fabric administrator authorises to certify.	☐	☒

Tick a box only when you could explain the point to someone else

☐ Tenant → capacity → workspace → item domains group workspaces	☐ F64+ for free viewers smoothing 5 min / 24 h, throttling 10 min / 60 min / 24 h
☐ Roles are workspace-wide; share items for least privilege Read, ReadData, ReadAll, Build, Reshare	☐ RLS filters only Viewers test with View as
☐ Each engine has its own row and column security SQL policy, DAX roles + OLS, OneLake security	☐ Labels flow downstream, endorsement builds trust Promoted, Certified, Master data

Q1 Which F SKU is the smallest that lets free-licence users view Power BI content?

A F64.

Q2 Throttling stage after 60 minutes of future overage?

A Interactive requests are rejected (background continues until 24 hours of overage).

Q3 Which workspace role can add Members but not delete the workspace?

A Member.

Q4 Which item permission lets an analyst build reports on a model without workspace access?

A Build (with Read) on the semantic model.

Q5 How do you hide a salary column from a semantic-model role?

A Object-level security (OLS) on the column, set in Tabular Editor or TMDL.

Q6 DAX function used in dynamic RLS?

A USERPRINCIPALNAME() (compared with a security table).

Q7 Which T-SQL feature masks e-mail addresses in a Fabric warehouse?

A Dynamic data masking: ADD MASKED WITH (FUNCTION = 'email()'), UNMASK to reveal.

Q8 Where do you see which item consumed the capacity at 10 am?

A The Microsoft Fabric Capacity Metrics app.

Q9 Who can certify an item?

A Users or groups the Fabric administrator enables in the certification tenant setting.