SYMBEEO

PUBLIC

SOLUTION DESIGN DOCUMENT

Hybrid and multi-cloud foundation for a typical buyer, applying SRA-CLD-001

Design document (HLD + LLD)

CAPABILITY	DOCUMENT	VERSION	DATE
Cloud	SDD-CLD-001	1.3	Nov 4, 2026

WRITTEN BY

Steve Phillips, Principal Data Center Architect

© 2026 Symbeeo. All rights reserved.

Document control

Document	SDD-CLD-001	Version	1.3
Issued	Nov 4, 2026	Status	Issued by Symbeeo
Classification	Public	Supersedes	1.2, Oct 10, 2026
Capability	Cloud	Author	Steve Phillips
Role	Principal Data Center Architect	Applies to	SRA-CLD-001 v1.1
Tested by	STP-CLD-001		
Credentials	CCSP, CCIE, AWS Certified Security – Specialty		
Approval	Approved by Edwin Ozer, Founder, Oct 10, 2026 (version 1.2). Version 1.3 issued by Symbeeo, Nov 4, 2026.		
Sign-off	"The customer's named representative signs this document before build; the practice lead signs it after."		

Contents

1 · Introduction 3
2 · Prerequisites 4
3 · Solution overview 4
4 · Logical design 5
5 · Physical design 6
6 · Migration 6
7 · Roles and deliverables 7
8 · Change control and reporting 7
9 · Security and lifecycle clauses 7

© 2026 Symbeeo. All rights reserved. · Public

> CONVENTIONS
>
> The reference architecture applied to one client with names, sizes and a migration plan. Client values are the typical buyer's from SRA-CLD-001 §1 [A] until the design workshop replaces them. Platform figures are from the provider documents cited in SRA-CLD-001 §9 [S]. A row with more than one tag is counted once: as a published figure if any tag is [S] or [S*], otherwise as an assumption if any tag is [A], otherwise as a design target.

Table 1. Revision history

Date	Version	Change
Sep 27, 2026	1.0	First issue.
Oct 7, 2026	1.1	Reissued with the practice set; no change.
Oct 10, 2026	1.2	Approval line now reads: approved by the Founder, issued by Symbeeo. Steve Phillips remains the author.
Nov 4, 2026	1.3	Wording correction: how the comparison is described.

1 · Introduction

1.1 Purpose.

Design for bringing the client's public-cloud accounts under one landing zone per cloud, connecting both sites to both clouds privately, and placing each workload by a recorded score. The client signs before build.

1.2 Goals.

120 workloads in public cloud by 2028 under SRA-CLD-001 R1–R18; no workload outage during the move of existing accounts into the new hierarchy; an exit plan and an audit archive the regulator can read.

1.3 Approach.

Phase 1 facilities, edge and circuits built; encryption and key rotation tested (STP-CLD-001 T10, T13). Phase 2 landing zone for the primary cloud built from code; capacity, addressing and failover to its hub tested (T8, T9, T11, T12); existing accounts enrolled one by one. Phase 3 the same for the secondary cloud; cloud-to-cloud link. Phase 4 cost dataset, placement scores, exit test, acceptance.

1.4 Platform decision.

Primary and secondary cloud: two of AWS, Microsoft Azure or Google Cloud, chosen by the comparison. On-premises extension: one of none, Azure Local, AWS Outposts or Google Distributed Cloud connected, chosen at the design workshop; default none. The design below uses neutral terms; the workshop keeps one column of this map and deletes the rest.

Table 2. Platform decision

Neutral term	AWS	Azure	Google Cloud
account	account	subscription	project
hierarchy node	organizational unit	management group	folder
root guardrail	service control policy	Azure Policy at root group	organization policy

© 2026 Symbeeo. All rights reserved. · Public

Neutral term	AWS	Azure	Google Cloud
network hub	Transit Gateway or Cloud WAN	Virtual WAN or hub VNet	Network Connectivity Center hub
dedicated port	Direct Connect dedicated	ExpressRoute Direct	Dedicated Interconnect

2 · Prerequisites

Table 3. Prerequisites

#	Prerequisite	Owner	Status
P1	Two carrier-neutral facilities selected, each on the providers' port lists	Symbeeo	open
P2	Metro fiber or waves from both sites to both facilities (SDD-NET-001)	Symbeeo	open
P3	Identity provider groups for every cloud role created	client	open
P4	Approved-jurisdiction list and SEAL level per data class, in writing	client	open
P5	Inventory of existing cloud accounts with owners and spend	client	open
P6	Workload list with data class, latency need and criticality	client	open
P7	IPv4 and IPv6 allocations confirmed free of overlap with existing accounts	client	open
P8	Cost centers and owners for the tag schema	client	open
P9	Change windows for account enrollment agreed	both	open

3 · Solution overview

3.1 Places [A].

Table 4. Places [A]

Place	Holds	Link to the rest
Site A pod, site B pod	private cloud per SDD-DC-001; regulated data no provider place meets P4 for	DCI (SDD-NET-001); metro to both facilities
Facility 1, facility 2	2 edge routers each; cross-connects to both clouds	metro fiber to both sites
Cloud 1, primary	90 workloads; two regions in the approved jurisdictions	2 × 10 Gbps dedicated per facility
Cloud 2, secondary	30 workloads; one region, second for tier 1	2 × 10 Gbps dedicated per facility

3.2 Sizing [A].

Four 10 Gbps ports per cloud, two per facility on different edge routers: 40 Gbps with all up, 20 Gbps after a facility loss, which keeps R6 (≥ 10 Gbps per site per cloud) at two sites. Ports move to 100 Gbps when a month's 95th percentile passes 60 % of a facility's capacity. The facility pair is chosen to satisfy the chosen provider's 99.99 % topology rules [S].

© 2026 Symbeeo. All rights reserved. · Public

4 · Logical design

4.1 Hierarchy, identical in both clouds.

Table 5. Hierarchy, identical in both clouds

Node	Holds	Guardrails beyond root
security	log archive, security tooling	deny deletion of logs
platform/identity	directory sync, break-glass	human access by group only
platform/connectivity	hub, resolvers, dedicated-port attachments	network changes by pipeline only
platform/management	monitoring, backup vaults, cost export	—
workloads/prod	one account per workload	deny public endpoints without exception record
workloads/nonprod	one account per workload	budget alarm per account
sandbox	time-boxed accounts	no connectivity to hub; auto-close 90 days
decommissioned	closed accounts pending deletion	deny all

4.2 Address plan [A].

Table 6. Address plan [A]

Block	Use
10.1.0.0/16 · 10.2.0.0/16	site A · site B (SDD-DC-001 §4.1)
10.64.0.0/12	cloud 1: /14 per region (256 × /22), /22 per workload account; 180 accounts (90 workloads × prod and nonprod) fit in either region
10.80.0.0/12	cloud 2: same scheme
10.255.0.0/24	facility transit, /31 per BGP session
client IPv6 /48	/56 per place, /64 per subnet

4.3 Identity.

SAML or OIDC from the client's identity provider to each cloud and to the private-cloud management plane; roles bound to groups (P3); two break-glass accounts per cloud with hardware keys, stored at the two sites, alarm on sign-in (R2).

4.4 Root guardrails.

Region allow-list from P4; deny public object storage; require encryption at rest with customer-managed keys for regulated data; deny disabling of the audit trail (R3, R4, R12). Held in the landing-zone repository; applied only by pipeline (R17).

4.5 Routing and encryption.

eBGP from each edge router to each cloud, private ASNs 64512–64515 for the four edge routers; ECMP across all sessions; BFD at 300 ms × 3, giving ≤ 1 s detection inside R9's 3 s. MACsec with 256-bit keys on every dedicated port, GCM-AES-XPN-256 on ports of 100 Gbps and above [S]; commissioned in should-encrypt, moved to must-encrypt

© 2026 Symbeeo. All rights reserved. · Public

after T10 passes; keychain holds current and previous key for rotation (R8). Cloud-to-cloud: provider-managed interconnect where the pair is offered [S]; otherwise via the facility edge (F7).

4.6 Names.

Inbound and outbound resolver endpoints in each cloud hub; on-premises DNS forwards the clouds' private zones to them, and they forward the client's internal zone back (R11).

4.7 Logging.

Organization audit trail of each cloud to the security account's write-once storage, retention 400 days, then archive tier (R12); copy streamed to the client's SIEM (SDD-SEC-001).

4.8 FinOps.

Mandatory tags on every resource: owner, cost-center, environment, data-class, placement-id. Each provider's FOCUS export and the private cloud's monthly cost model loaded daily into one dataset (R13); showback per owner monthly. The placement score (R14) weighs 3-year cost, latency to users, residency and SEAL fit, and exit effort, 25 % each [A].

4.9 Recovery and exit.

Tier-1 workloads: replication to a second region of the same cloud or to a pod, RPO 15 min, RTO 4 h (R16). Each critical workload's exit plan names the target place, the export format per data store and the 30-day transition timetable (R15).

5 · Physical design

Per facility: 2 edge routers, each with MACsec-capable 10/100G ports, single-mode LR optics to the providers' specification [S], A/B power, one out-of-band line; cross-connects ordered by letter of authorization from each provider. Elevations and cross-connect IDs recorded in the as-built.

6 · Migration

Table 7. Migration

Step	Action	Rollback
1	Build facilities, edge and circuits to both clouds; run STP-CLD-001 T10 and T13 on every dedicated port	—
2	Build primary landing zone from code; run T1–T7, T14, T16, T22, T23 on an empty workload account, and T8, T9, T11, T12 to its hub	destroy and re-apply
3	Enroll existing accounts one per window: move into hierarchy, apply guardrails, re-address if P7 found overlap; T21 on the first	move account back to its old node
4	Build secondary landing zone; repeat T1–T7, T14, T16, T22, T23 there, and T8, T9, T11, T12 to its hub; cloud-to-cloud link, T15	—
5	Cost dataset, tags, placement scores; T17–T18	—
6	Tier-1 failover and one exit test; T19–T20; acceptance	fail back

© 2026 Symbeeo. All rights reserved. · Public

7 · Roles and deliverables

Design authority: practice lead (signs) and client cloud platform owner (signs). Deliverables: this document · STP-CLD-001 with results · landing-zone repository · as-built (ports, cross-connect IDs, ASNs, prefixes, versions) · exit plans · acceptance certificate.

8 · Change control and reporting

8.1 Change orders.

Once this document is signed, any change to it is a written change order stating what changes, why, and its effect on cost and schedule. Both design authorities (§7) sign it before the change is built. A change built without a signed order is not accepted under STP-CLD-001.

8.2 Weekly status report.

Every week of the build the implementation lead sends the client's cloud platform owner: % complete per deliverable in §7, slippage against the phase plan in §1.3 (days, per phase).

8.3 Escalation contacts, named at the workshop.

Table 8. Escalation contacts, named at the workshop

Level	Symbeeo	Client
1 · day to day	implementation lead	cloud platform owner
2 · slippage > 5 working days or a disputed change order [A]	practice lead	head of infrastructure
3 · unresolved at level 2 after 5 working days [A]	the Founder	the client's executive sponsor

9 · Security and lifecycle clauses

9.1 Incidents.

A security incident affecting the client's data or systems (any account, circuit, edge device or pipeline in scope) is reported to the client's named security contact within 24 hours of its discovery.

9.2 Media sanitization.

Storage media leaving the client's control — edge-router flash and disks on return, RMA or retirement, and any on-premises extension hardware (D3 in SRA-CLD-001 §5) returned to its provider — are sanitized to NIST SP 800-88 Rev. 2 (final, September 2025, superseding Rev. 1 [S], read Sep 24, 2026 at `https://csrc.nist.gov/pubs/sp/800/88/r2/final`), with a certificate per device. Where the provider sanitizes its own returned hardware, its per-device record is obtained and filed with the handover pack [A]. Media may instead stay with the client under a non-return service; media holding PHI or other regulated personal data are never taken back unsanitized.

9.3 End of sale and end of support.

No equipment (edge routers, optics, on-premises extension hardware) is quoted past its vendor's end-of-sale date, and every quote shows the end-of-support date of every item. Cloud services are quoted only where the provider has not

© 2026 Symbeeo. All rights reserved. · Public

announced their retirement [A].

9.4 Support levels.

Every quote states the vendor support level by severity: the response time for severity 1 to 4, for each cloud provider's support plan, each carrier circuit and each edge-router support contract. Figures are taken from the vendor's contract at quote time, not from this document.

9.5 Handover pack.

At acceptance the client receives: as-built drawings (facility elevations, cross-connect IDs, circuit IDs, ASNs, prefixes); configurations (edge routers and the landing-zone repository at its final tag); credentials transferred, including the break-glass accounts' hardware keys (§4.3); licenses; support contracts; STP-CLD-001 signed; and open items with owner and date.

© 2026 Symbeeo. All rights reserved. · Public

SYMBEEO

Each vendor's tool shows you their option. We show you all of them against one requirement.

Compared. Then Delivered.

hello@symbeeo.com · symbeeo.com

© 2026 Symbeeo. All rights reserved.

Product and company names and logos are their owners' trademarks, shown only to identify the lines Symbeeo sources. Naming a vendor or showing its logo does not mean the vendor sponsors or approves Symbeeo's comparisons or any recommendation Symbeeo makes.

Figures are as published by their sources on the dates given in this document; figures marked [A] are assumptions.

SDD-CLD-001 · Version 1.3 · Nov 4, 2026