SYMBEEO

PUBLIC

REFERENCE ARCHITECTURE

Hybrid and multi-cloud foundation on 2026 platforms: landing zones, private connectivity, sovereign placement, FinOps

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

WRITTEN BY

Steve Phillips, Principal Data Center Architect

© 2026 Symbeeo. All rights reserved.

Document control

Document	SRA-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	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 practice lead signs this document before any build proceeds under it."		

Contents

1 · Scope 3
2 · Requirements register 3
3 · Architecture overview 5
4 · Component design 5
5 · Options and platform choices 6
6 · Failure conditions 7
7 · Validation 8
8 · Operations and lessons learned 8
9 · Appendix 8

© 2026 Symbeeo. All rights reserved. · Public

CONVENTIONS

Source tags. [S] read Sep 24, 2026 from the publisher's own document (provider documentation, release notes, standards bodies; list with URLs in §9) · [S*] secondary source, used only where the primary was not read · [A] typical-buyer assumption · [CMP] the row a comparison decides; none for this capability is published or numbered yet. 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	Three rules removed from the §9.1 table of industry rules.
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 · Scope

Who it is for. The head of infrastructure who runs a private cloud (SRA-DC-001), has workloads drifting into public clouds account by account, and must show the board and the regulator that every account sits under one set of controls, that placement was decided on numbers, and that any provider can be left on the EU Data Act's timetable.

Typical buyer [A]. The SRA-DC-001 typical buyer, extended: two sites 40 km apart, each with a private-cloud pod; one primary public cloud and one secondary; 120 workloads placed in public cloud by 2028; EU-resident regulated data; a single identity provider; a regulator that asks for the exit plan and the audit log, not a description of them.

What is in. The landing zone in each public cloud (organization hierarchy, identity, guardrails, logging); private connectivity from both sites to each cloud and between clouds; address and name plan across all places; on-premises extensions of a public cloud; sovereign placement; FinOps data and the placement decision; exit. **What is out.** The private-cloud pods themselves (SRA-DC-001); the WAN, campus and DCI (SRA-NET-001); zero-trust user access (SRA-SEC-001); GPU clusters (SRA-AI-001); application refactoring.

Related documents. SDD-CLD-001 applies this document; STP-CLD-001 tests it. Sources in §9.

2 · Requirements register

Each row is tested in STP-CLD-001 and names no product; products are §5.

Table 2. Requirements register

#	Requirement	Value	Source
R1	Environment isolation	0 accounts, subscriptions or projects holding more than one environment (production, non-production, sandbox) of a workload	[S]

© 2026 Symbeeo. All rights reserved. · Public

#	Requirement	Value	Source
R2	Identity	100 % of human sign-ins to every cloud and the private cloud authenticated by one identity provider, except ≤ 2 alarmed break-glass accounts per cloud	[S]; [A]
R3	Preventive guardrails	the root guardrail set (region allow-list, public-storage denial, encryption at rest) in force on 100 % of accounts before their first workload	[S]
R4	Data residency	0 copies of regulated data (primary, backup, log) outside the client's approved jurisdictions	[A]
R5	Sovereignty assurance	every provider holding regulated data assessed at or above the client's SEAL level under the EU Cloud Sovereignty Framework v1.2.1; typical buyer SEAL-2	[S]; [A]
R6	Private capacity, per site per cloud	≥ 10 Gbps committed	[A]
R7	Connectivity resilience	every site keeps a path to every cloud after the loss of any one circuit, edge device or facility	[S]
R8	Encryption on private circuits	100 % of traffic between client edge and cloud edge encrypted with AES-256	[S]
R9	Path failover	traffic moved to the surviving path ≤ 3 s after a circuit loss	[A]
R10	Address plan	one IPv4/IPv6 plan across sites and clouds; 0 overlapping prefixes	[S]
R11	Name resolution	private names resolve in both directions between every site and every cloud	[S]
R12	Audit logging	control-plane logs of 100 % of accounts held in one write-once archive for ≥ 400 days	[S]; [A]
R13	Cost allocation	≥ 95 % of each month's cloud and private-cloud spend allocated to a named owner in one dataset conforming to FOCUS 1.2 or later	[S]; [A]
R14	Placement decision	100 % of workloads carry a placement score (3-year cost, latency, residency, exit effort) recorded before build	[S]; [A]
R15	Exit	every critical workload's exit plan tested in the last 12 months, its data exported in documented open formats within 30 days	[S*]
R16	Recoverability, tier 1	RPO 15 min, RTO 4 h, to a second region or a pod	[A]

© 2026 Symbeeo. All rights reserved. · Public

#	Requirement	Value	Source
R17	Declared state	100 % of landing-zone resources match version-controlled code, checked every 24 h	[S]
R18	Account vending	account with R1–R3 and R12 applied delivered ≤ 1 working day after approval	[A]

3 · Architecture overview

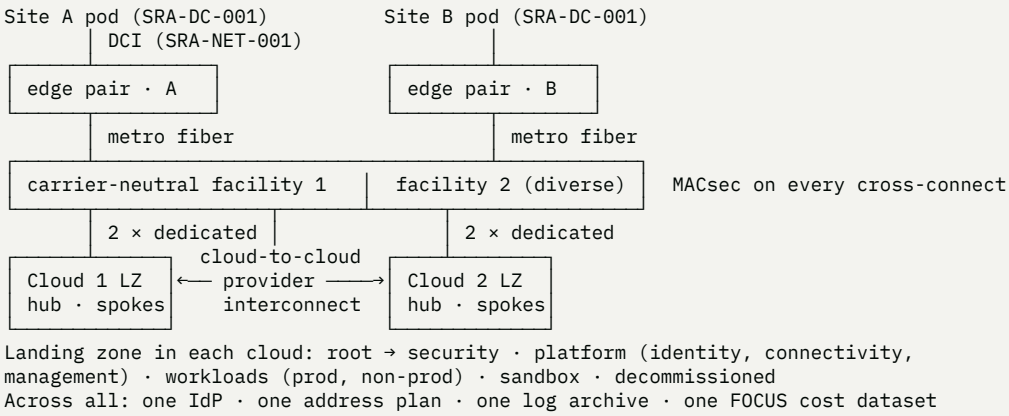


Figure 1. Landing zones and private connectivity to two clouds

4 · Component design

4.1 Landing-zone hierarchy.

One organization per cloud, one shape in all: security, platform (identity, connectivity, management), workloads (production, non-production), sandbox, decommissioned. AWS Control Tower landing zone 4.0 makes the structure and its Config and CloudTrail integrations optional and dedicated [S]; the Azure landing zones library adds a Security management group and, in 2026.04.2, a Local group for Azure Local and Arc estates [S*]; Google's enterprise foundations blueprint uses environment folders with Shared VPC [S]. R1, R18.

4.2 Identity.

One identity provider federated by SAML or OIDC into every cloud and the private-cloud management plane; groups carry roles; break-glass accounts offline and alarmed (R2).

4.3 Guardrails.

Preventive policy at the root (R3, R4), detective policy per account, both as code (R17), mapped to CSA CCM v4.1 [S].

4.4 Connectivity.

Two carrier-neutral facilities, each with a client edge pair and dedicated ports to each cloud; one hub per cloud, spokes per workload account. MACsec (IEEE 802.1AE) on every dedicated port: AWS Direct Connect supports it at 10, 100 and 400 Gbps, requiring GCM-AES-XPN-256 at 100 and 400; Azure ExpressRoute Direct offers 10, 100 and 400 Gbps port pairs; Google Cloud Interconnect supports it on listed circuits [S]. A partner-hosted circuit carries IPsec instead (R8).

© 2026 Symbeeo. All rights reserved. · Public

BGP with BFD on every session (R9). Cloud-to-cloud uses a provider-managed link where offered: AWS Interconnect – multicloud, generally available April 14, 2026 with Google Cloud, MACsec on by default, 1–100 Gbps, four links over two facilities; Oracle Cloud Infrastructure generally available since July 2026 and Microsoft Azure in preview since August 31, 2026 [S] (AWS What's New, checked Sep 26, 2026: `https://aws.amazon.com/about-aws/whats-new/2026/07/aws-announces-AWS-interconnect-multicloud-OCI-GA/` · `https://aws.amazon.com/about-aws/whats-new/2026/08/aws-announces-AWS-interconnect-multicloud-microsoft-azure-preview/`).

4.5 Addressing and names.

One plan from non-overlapping supernets, held in one IPAM (R10); resolver endpoints in each cloud hub, conditional forwarding on-premises (R11).

4.6 On-premises extension and sovereign places.

Placed per data class (R4, R5): the private-cloud pods (SRA-DC-001; the VCF path is at 9.1.1, GA September 3, 2026 [S]); a provider control plane on hardware in the client's rack — Azure Local (current release 12.2609.1003.7, September 2026; rack-aware clustering and disconnected operations available), AWS Outposts second generation (single 42U rack announced September 2026), Google Distributed Cloud connected or air-gapped [S]; or a sovereign region such as the AWS European Sovereign Cloud (generally available January 15, 2026) [S]. Each placement is assessed on the framework's eight objectives, SOV-1 to SOV-8, with a SEAL level per objective set by the assessing buyer, as the framework's contracting authority does [S] (framework v1.2.1, §1 and §4, read Sep 27, 2026); in a design study or design the levels are our own assessment [A] until the client signs them.

4.7 Logging.

Organization-wide audit trail to the security account's write-once store (R12); posture findings forwarded to the client's SIEM (SRA-SEC-001).

4.8 FinOps and placement.

Provider cost exports in FOCUS form (1.4, ratified June 4, 2026, adds the Invoice Detail and Billing Period datasets; 1.2 set as the floor [A]) and the private-cloud cost model in one dataset (R13). The FinOps Framework 2026 brings data center and AI spend into the same scopes as public cloud, which makes a like-for-like placement score possible (R14) [S].

4.9 Resilience and exit.

Tier-1 workloads replicate to a second region or a pod (R16). Exit plans follow the Data Act switching chapter, applicable since September 12, 2025: at most two months' notice, a 30-day transitional period, switching charges abolished from January 12, 2027 [S*] (R15).

4.10 Lifecycle.

Landing zones, network and policy declared in OpenTofu or Terraform through a reviewed pipeline (R17); container platforms on a Kubernetes minor in upstream support (1.36, April 22, 2026) [S].

5 · Options and platform choices

One row per decision. Every option weighed is kept, rejected ones included, with whether it meets §2 and its cost band.

© 2026 Symbeeo. All rights reserved. · Public

Table 3. Options and platform choices

ID	Decision	Requirement	Alternatives considered	Decision taken	Rationale
D1	Primary and secondary public cloud	R1–R18	AWS · Microsoft Azure · Google Cloud; all meet §2; consumption-priced	[CMP]	All three publish a landing-zone shape, MACsec private ports and FOCUS exports [S]; the choice between them is the comparison's
D2	Landing-zone tooling	R1, R3, R17, R18	provider's own: Control Tower 4.0 + Landing Zone Accelerator · ALZ library via Terraform/Bicep · enterprise foundations blueprint / Cloud Foundation Fabric; meets §2; included in the platform	the provider's own, per cloud	Provider-maintained; drift follows provider releases [S]
D3	On-premises extension of a public cloud	R4, R5	Azure Local · AWS Outposts 2nd gen · Google Distributed Cloud connected; meet §2; subscription or rack lease — none, SRA-DC-001 pods only; meets §2; no added cost	none by default; [CMP] only if the primary cloud's services are needed on-site	The private cloud is already sized for the estate [A]; an extension puts the provider's control plane in the client's rack [S]
D4	VMware estate into public cloud	R14, R15	Amazon EVS · Azure VMware Solution · Google Cloud VMware Engine · Nutanix NC2 (AWS, Azure, Google Cloud since January 2026); meet §2; node-priced	per client, by placement score	Moves VMs without refactoring [S]; exit effort is scored in R14
D5	Cloud-to-cloud path	R7, R8	provider-managed interconnect; meets §2 where offered; priced per Gbps — hairpin through the facility edge, or a virtual router in an interconnection fabric; meets §2; ports + cross-connects	provider-managed where the pair is offered; facility edge as fallback	Fewer parts, MACsec by default [S]; the fallback works for any pair but adds latency
D6	Site-to-cloud connectivity	R6, R7, R8, R9	two facilities, dedicated ports to each cloud (§4.4) — single facility, single circuit per cloud: fails R7; lower cost — site-to-cloud IPsec over internet only: fails R6, R9; lowest cost	two facilities, dedicated ports	One cut isolates a cloud in the single-facility design; over the internet, throughput and failover cannot be committed

6 · Failure conditions

Table 4. Failure conditions

#	Condition	What the user sees	Recovers by itself	Needs a hand	Time
F1	One dedicated circuit down	none	BGP/BFD moves traffic	carrier repair	≤ 3 s (R9)
F2	One facility lost	none; half capacity	second facility carries all	restore facility	≤ 3 s
F3	MACsec key mismatch after rotation	none if keychain holds previous key	falls back to previous key	correct key	0
F4	Cloud region impaired	tier-1 workloads down until failover	no	run recovery plan	RTO 4 h (R16)
F5	Identity provider unreachable	no new sign-ins	no	break-glass per cloud	minutes

© 2026 Symbeeo. All rights reserved. · Public

#	Condition	What the user sees	Recovers by itself	Needs a hand	Time
F6	Guardrail removed or drifted	none	no	pipeline re-applies	≤ 24 h (R17)
F7	Cloud-to-cloud interconnect down	cross-cloud calls slower	traffic hairpins through facility	provider repair	seconds
F8	Provider exit triggered	none during transition	no	run exit plan	≤ 30 days (R15)

7 · Validation

None yet. STP-CLD-001 is the test plan; run on the first build and recorded here, it makes this document a validated architecture.

8 · Operations and lessons learned

Monthly FinOps review against R13; yearly placement review (R14) and exit test (R15); quarterly circuit failover test; landing-zone library upgrades within 90 days of a provider release [A]. Lessons: to be written by the signing engineer.

9 · Appendix

Ordering list, per cloud [S]/[A]: 2 × dedicated ports per facility (four per cloud, SDD-CLD-001 §3.2) · 2 × edge routers per facility with MACsec-capable 100G ports · cross-connects · landing-zone account set (security, log archive, identity, connectivity, management) · FOCUS export enabled · support plan.

References, read Sep 24, 2026 unless marked in the text. AWS Interconnect GA, Apr 14, 2026 — https://aws.amazon.com/blogs/aws/aws-interconnect-is-now-generally-available-with-a-new-option-to-simplify-last-mile-connectivity/ · AWS Direct Connect MACsec — https://docs.aws.amazon.com/directconnect/latest/UserGuide/MACsec.html · Azure ExpressRoute Direct — https://learn.microsoft.com/en-us/azure/expressroute/expressroute-erdirect-about · Google Cloud Interconnect — https://docs.cloud.google.com/network-connectivity/docs/interconnect/concepts/overview · AWS Control Tower LZ 4.0 — https://docs.aws.amazon.com/controltower/latest/userguide/key-changes-lz-v4.html · Azure landing zones, what's new — https://azure.github.io/Azure-Landing-Zones/whats-new/ · ALZ Local management group [S*] — https://www.azurecitadel.com/blog/2026-04-29-slz-2026-04-2 · Google enterprise foundations blueprint — https://docs.cloud.google.com/architecture/blueprints/security-foundations · Azure Local, what's new — https://learn.microsoft.com/en-us/azure/azure-local/whats-new · AWS Outposts second generation — https://aws.amazon.com/about-aws/whats-new/2025/04/second-generation-aws-outposts-racks/ and https://aws.amazon.com/about-aws/whats-new/2026/09/single-rack-aws-outposts/ · Google Distributed Cloud — https://cloud.google.com/distributed-cloud · VCF 9.1.1 — https://blogs.vmware.com/cloud-foundation/2026/09/03/announcing-general-availability-of-vmware-cloud-foundation-9-1-1/ · Amazon EVS — https://aws.amazon.com/about-aws/whats-new/2025/08/aws-general-availability-amazon-elastic-evs · Nutanix NC2 on Google Cloud — https://www.nutanix.com/blog/announcing-nutanix-cloud-clusters-nc2-on-google-cloud · AWS European Sovereign Cloud — https://press.aboutamazon.com/aws/2026/1/aws-launches-aws-european-sovereign-cloud-and-announces-expansion-across-europe · EU Cloud Sovereignty Framework v1.2.1 — https://commission.europa.eu/document/download/09579818-64a6-4dd5-9577-446ab6219113_en · EU Data Act switching [S*] — https://www.garrigues.com/en_GB/garrigues-digital/data-act-and-cloud-switching-keys-new-rules-changing-cloud-service-providers · FOCUS 1.4 — https://focus.finops.org/focus-specification/ · FinOps Framework 2026 —

© 2026 Symbeeo. All rights reserved. · Public

https://www.finops.org/insights/2026-finops-framework/ · CSA CCM v4.1 — https://cloudsecurityalliance.org/artifacts/cloud-controls-matrix-v4-1 · Kubernetes 1.36 — https://kubernetes.io/blog/2026/04/22/kubernetes-v1-36-release/

Watched, not relied on. Post-quantum key exchange for IKEv2 with ML-KEM is still an IETF draft (draft-ietf-ipsecme-ikev2-mlkem, February 2026), so R8 names AES-256 and not a key-exchange algorithm — https://datatracker.ietf.org/doc/html/draft-ietf-ipsecme-ikev2-mlkem-04

9.1 · Industry rules this architecture helps a buyer meet.

From Symbeeo's industry research of September 2026. Only rules that research links to this document's requirements are listed; rules it found this document does not address are left out.

Table 5. Industry rules this architecture helps a buyer meet

Rule	Jurisdiction	What it asks of infrastructure	Requirements here	Coverage
SEC Rule 17a-4 (17 CFR 240.17a-4), as amended 2022	US · broker-dealers	records preserved on write-once media, or with an audit trail that recreates any modified or deleted record	R12	partial
21 CFR Part 11 (electronic records; electronic signatures)	US · FDA-regulated records	secure audit trails kept as long as the records	R12	partial
EU GMP Annex 11 Computerized Systems (2011 revision in force; the 2025 revision draft is not final)	EU · medicinal-product manufacturers	audit trails and archiving of GMP records	R12	partial
US state comprehensive privacy laws (23 states with signed laws, IAPP tracker updated Sep 8, 2026)	US · states	reasonable security and control over where personal data is held	R4	partial

Naming a rule here is not a claim of compliance or certification: the buyer's assessor decides compliance, and Symbeeo holds no certification or authorization.

Sources for §9.1, read Sep 25, 2026: SEC Rule 17a-4 amendments [S] https://www.federalregister.gov/documents/2022/11/03/2022-22670/electronic-recordkeeping-requirements-for-broker-dealers-security-based-swap-dealers-and-major · 21 CFR Part 11 [S] https://www.ecfr.gov/current/title-21/chapter-I/subchapter-A/part-11 (text read on the eCFR) · EudraLex Volume 4, Annex 11 [S] https://health.ec.europa.eu/medicinal-products/eudralex/eudralex-volume-4_en · IAPP US State Privacy Legislation Tracker [S] https://iapp.org/resources/article/us-state-privacy-legislation-tracker/.

© 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.

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