Twenty connector configuration

This reference describes the product settings accepted by aip-host-twenty at the reviewed source revision. A complete deployment combines them with the shared connector-host identity, PostgreSQL, routing, signing, lifecycle, and optional ca

SECTION	Connectors
TYPE	Connector
PROTOCOL	AIP 1.0
SOURCE	docs/connectors/twenty/reference/configuration.md

Twenty product settings are read when the host process starts. Only the shared non-secret credential-revision policy is re-read before provider side effects.

Configuration identity

Property	Value
Host binary	`aip-host-twenty`
AIP workspace version	`1.0.0`
Reviewed AIP source	`97be86e9efedf07ecf1783b03800f683f107fb04`
Connector ID	`twenty`
Connector profile	`aip.connector.twenty.v1`
Provider mapping revision	`96a24563674313a3071d359bfccaf33d5e130ab8`
Capability prefix	`cap:twenty:`

The provider revision identifies the source used to derive the fixed mapping. It does not establish compatibility with an unpinned provider deployment.

Configure the Twenty host

Environment variable	Command-line flag	Required	Default	Meaning
`AIP_TWENTY_BASE_URL`	`--base-url`	Yes	None	Fixed provider origin
`AIP_TWENTY_WORKSPACE_ID`	`--workspace-id`	Yes	None	Fixed workspace UUID
`AIP_TWENTY_API_TOKEN_FILE`	`--api-token-file`	Yes	None	Owner-controlled provider token file
`AIP_TWENTY_WEBHOOK_SECRET_FILE`	`--webhook-secret-file`	No	None	Owner-controlled webhook HMAC secret; omission disables ingress
`AIP_TWENTY_ALLOW_INSECURE_HTTP`	`--allow-insecure-http`	No	`false`	Permit HTTP for an explicitly trusted private network
`AIP_TWENTY_MAX_RESPONSE_BYTES`	`--max-response-bytes`	No	`67108864`	Maximum accepted provider response
`AIP_TWENTY_OPERATIONS_FILE`	`--operations-file`	No	All 22 operations	JSON array of admitted capability suffixes

All command-line forms are process arguments. Prefer environment values and file-backed secrets in deployment configuration; never pass secret bytes as a command-line value.

Validate the provider origin

The base URL must contain a host and no username, password, path other than empty or `/`, query, or fragment. HTTPS is required by default.

Loopback HTTP is accepted without the explicit private-network switch. Other HTTP origins require `AIP_TWENTY_ALLOW_INSECURE_HTTP=true`. The switch does not disable host validation or enable provider redirects.

The connector joins only fixed route templates to this origin. Configure an origin rather than an application path prefix.

Validate the workspace and token

`AIP_TWENTY_WORKSPACE_ID` accepts a canonical 36-character RFC 4122 UUID with version 1 through 5 and an RFC variant nibble. The value scopes deterministic create IDs and must match each accepted webhook payload's `workspaceId`.

The API token file is read through the shared bounded-secret reader:

- regular files only;
- no symlinks;
- no group or world permission bits on Unix;
- same inspected and opened file identity;
- non-empty UTF-8 after surrounding ASCII whitespace is trimmed;
- maximum 16 KiB;
- temporary string zeroization after connector construction.

The connector adds the token as a provider `Authorization: Bearer` header. Capability input cannot override it.

Restrict the operation catalogue

The optional operations file is a JSON array of capability suffix strings. It is read as non-secret configuration with a 128 KiB ceiling.

```
JSON
[
  "record.list",
  "record.get",
  "record.create",
  "openapi.core"
]
```

Every suffix must be one of the connector's 22 operations. Unknown values fail startup. Duplicate values collapse into one set, while an empty resulting set is invalid.

Omission enables all 22 operations in the connector instance. Registry policy can narrow routing further, but it cannot make the process execute an operation absent from this file.

Changing the file does not change a running host. Replace the replica and re-admit the resulting manifest and route identity.

Set the response bound

`AIP_TWENTY_MAX_RESPONSE_BYTES` accepts `1` through `268435456`. Omission uses `67108864` bytes.

The connector rejects a declared `Content-Length` above the bound and stops accumulating a streamed response when the bound would be exceeded. An empty response becomes JSON `null`; non-empty bytes must decode as JSON.

The configured response limit is published in the connector manifest. It does not increase provider request, webhook body, native envelope, PostgreSQL, or ingress limits.

Configure webhook ingress

Webhook ingress is disabled when `AIP_TWENTY_WEBHOOK_SECRET_FILE` is absent. When present, the host also requires `AIP_CONNECTOR_HOST_EVENT_ENDPOINT` and constructs the route `/webhooks/twenty`.

The webhook secret uses the 16 KiB shared secret-file bound. The ingress body limit is fixed at 4 MiB. Clock skew is fixed at 300,000 ms, and the durable replay window holds at most 100,000 live nonces.

Relevant common event settings are:

Setting	Default	Role
`AIP_CONNECTOR_HOST_EVENT_ENDPOINT`	None	Fixed central connector-event ingress
`AIP_CONNECTOR_HOST_EVENT_ALLOW_HTTP`	`false`	Permit controlled HTTP callback transport
`AIP_CONNECTOR_HOST_EVENT_ALLOW_PRIVATE`	`false`	Permit a controlled private destination

The product secret alone is insufficient. Event publication also depends on shared host signing, identity, durable outbox, and central ingress policy.

Apply shared host identity and route settings

The global host reference owns the exhaustive common matrix. These groups are required for Twenty behavior.

Identity and admission

Setting	Role
`AIP_CONNECTOR_HOST_PUBLIC_ENDPOINT`	Reachable native endpoint ending in `/aip/v1/messages`
`AIP_CONNECTOR_HOST_TYPE_ID`	Admitted Twenty connector type
`AIP_CONNECTOR_HOST_VERSION_ID`	Immutable admitted version
`AIP_CONNECTOR_HOST_INSTANCE_ID`	Logical runtime and webhook replay scope
`AIP_CONNECTOR_HOST_REPLICA_ID`	Concrete process identity
`AIP_CONNECTOR_HOST_TENANT_ID`	Verified tenant owned by the instance
`AIP_CONNECTOR_HOST_MEMBERSHIP_ID`	Stable membership assertion
`AIP_CONNECTOR_HOST_ARTIFACT_DIGEST`	Exact host artifact digest
`AIP_CONNECTOR_HOST_SECRET_PROVIDER_REF`	Non-secret provider reference
`AIP_CONNECTOR_HOST_CONFIG_REVISION`	Monotonic configuration revision; default `1`

Optional external-account ID and system must appear together. The common host does not compare the external-account ID with the Twenty workspace UUID.

PostgreSQL, signing, and lifecycle

Setting	Required or default
`AIP_CONNECTOR_HOST_BIND`	Default `0.0.0.0:8081`
`AIP_CONNECTOR_HOST_DATABASE_URL_FILE`	Required owner-controlled PostgreSQL URL
`AIP_CONNECTOR_HOST_SIGNING_SEED_FILE`	Required owner-controlled Ed25519 seed
`AIP_CONNECTOR_HOST_CONTROL_ENDPOINT`	Required lifecycle endpoint
`AIP_CONNECTOR_HOST_CONTROL_DID` or `_FILE`	Exactly one control-plane DID source
`AIP_CONNECTOR_HOST_GATEWAY_PRINCIPAL_ID`	Required trusted gateway principal
`AIP_CONNECTOR_HOST_GATEWAY_DID` or `_FILE`	Exactly one gateway DID source
`AIP_CONNECTOR_HOST_TRUST_DOMAIN`	Required trust domain
`AIP_CONNECTOR_HOST_TLS_CA_FILE`	Optional private-PKI root
`AIP_CONNECTOR_HOST_MAX_IN_FLIGHT`	Default `32`
`AIP_CONNECTOR_HOST_LEASE_TTL_MS`	Default `30000`
`AIP_CONNECTOR_HOST_HEARTBEAT_MS`	Default `10000`
`AIP_CONNECTOR_HOST_DRAIN_TIMEOUT_MS`	Default `30000`
`AIP_CONNECTOR_HOST_HEALTH_TIMEOUT_MS`	Default `2000`
`AIP_CONNECTOR_HOST_CONTROL_TIMEOUT_MS`	Default `5000`

Shared credential ID, issuer, scopes, revision, and revision-policy settings are optional as one complete unit. They fence route authorization but do not replace the Twenty API token or webhook secret.

Topology and callbacks

Setting	Default
`AIP_CONNECTOR_HOST_REGION`	`global`
`AIP_CONNECTOR_HOST_ZONE`	`default`
`AIP_CONNECTOR_HOST_CAPACITY_CLASS`	`standard`
`AIP_CONNECTOR_HOST_CALLBACK_ENDPOINT`	None
`AIP_CONNECTOR_HOST_CALLBACK_ALLOW_HTTP`	`false`
`AIP_CONNECTOR_HOST_CALLBACK_ALLOW_PRIVATE`	`false`

The connector exposes synchronous, non-streaming operations. A stream callback is not required by the Twenty operation contracts at this revision.

Use the effective limits

Boundary	Reviewed value
Provider HTTP connect timeout	10 seconds
Provider HTTP total timeout	120 seconds
Provider request JSON	16 MiB
Provider response, default	64 MiB
Provider response, maximum	256 MiB
Webhook request body	4 MiB
Webhook timestamp skew	300,000 ms
Live webhook replay nonces	100,000
Operation configuration file	128 KiB
API-token or webhook-secret file	16 KiB
Bulk record count	200
Object identifier	128 bytes
Query entries	64
Query value	32 KiB
Mutation idempotency key	1 through 1,024 ASCII graphic bytes

The effective ceiling is the smallest applicable bound. Raising the response limit does not enlarge requests, webhook bodies, record batches, query values, native envelopes, or shared host limits.

Understand readiness

The connector sends authenticated `GET /rest/open-api/core` to the configured origin. Any successful HTTP status reports the provider workspace API as reachable; transport or non-success status fails the connector health check.

Common host readiness also depends on PostgreSQL, the registry lease, lifecycle state, route identity, and other shared controls.

Readiness does not verify every admitted operation, mutation permission, idempotency behavior, webhook signature, event publication, replay recovery, custom object schema, or provider revision.

Know startup and reload ownership

Value	Read
Origin, workspace, API token, webhook secret	Host startup
Response limit and operation file	Host startup
Shared identity, storage, endpoints, and lifecycle limits	Host startup
Webhook replay scope	Constructed from instance ID at startup
Credential-revision policy file	Startup, then before provider side effects

Change startup-owned values through a controlled replica replacement. Editing a mounted operation, token, secret, or identity file does not update a running connector, manifest, replay scope, or route assignment.

Diagnose configuration failures

Failure	First decision
Origin is rejected	Supply an allowed origin with no credentials, path, query, or fragment
Workspace is rejected	Supply a canonical RFC 4122 UUID version 1 through 5
Token or webhook file is rejected	Check regular-file type, permissions, UTF-8, size, and content without printing it
Response limit is rejected	Choose `1` through `268435456` bytes
Operation file is rejected	Check its 128 KiB bound, JSON array shape, known suffixes, and non-empty set
Webhook secret is configured but startup fails	Configure an authorized central event endpoint and its trust material
Host remains unready	Check authenticated core OpenAPI reachability, PostgreSQL, lease, and lifecycle state
Provider returns a redirect	Correct the fixed origin or provider routing; redirects are disabled
Credential revision is denied	Repair policy or roll to an authorized revision before enabling provider work

Related documentation

- Twenty connector overview
- Authentication and workspace isolation
- Connector host configuration
- Connector host lifecycle
- Environment variables