Refine — GovCloud Setup Guide

For the broader architectural context (where the Refine server lives, network topology choices, cross-partition data flow), see `NETWORK_ARCHITECTURE.md`. For fully air-gapped GovCloud deployments (no NAT, VPC endpoints only), see `AIR_GAPPED_SETUP_GUIDE.md`.

Directory Integration in GovCloud

Directory provider	Works in GovCloud?	Notes
LDAP / on-prem AD	Yes	Same flow as commercial. AD must be reachable from the Refine VPC via VPN/peering/Direct Connect. See `LDAP_SETUP_GUIDE.md`.
Azure AD (commercial tenant)	Yes — only with NAT egress (Topology B)	Refine reaches `login.microsoftonline.com` over public internet. Won't work in air-gapped GovCloud (Topology D).
Azure AD (Government tenant — `*.onmicrosoft.us`)	Yes — only with NAT egress	Set Cloud=`government` in the Refine Directory Settings form. Endpoint becomes `login.microsoftonline.us`. v2.19+ supports this.
Local accounts only	Yes (always)	Skip directory integration; create users manually in Refine.

---

1. Overview

AWS GovCloud (US) is an isolated AWS partition designed for sensitive workloads subject to U.S. government compliance requirements (ITAR, FedRAMP, DoD, etc.). GovCloud accounts operate in a separate partition (`aws-us-gov`) and do not have access to commercial AWS services like Cost Explorer.

Refine supports GovCloud through a **dual-account architecture**:

- **GovCloud account** — where your regulated resources (EC2, RDS, etc.) run. Refine collects inventory from this account.
- **Linked commercial account** — the standard AWS account that is linked to your GovCloud account. Refine collects cost and billing data from this account via Cost Explorer.

Both accounts are added to Refine and linked together. Each gets its own CloudFormation stack, IAM credentials, and S3 bucket. Refine automatically associates cost data from the commercial account with resources discovered in GovCloud.

What You Get

Refine analyzes **13 services in GovCloud** (14 in the linked commercial account — Cost Explorer is not available in GovCloud) and provides:

- **Rightsizing recommendations** with ready-to-run CLI commands for EC2, RDS, and more
- **Exemptions** — mark resources as intentionally sized; exempt resources are excluded from future recommendations

- **Active Savings Plans tracking** — monitor utilization, coverage, and expiration (managed in the commercial account)
- **Savings Report** — unified view of realized and projected savings across both accounts
- **Cost Cleanup** — identify orphaned EBS snapshots, unused volumes, idle NAT gateways, and other waste
- **System Events** — audit log of syncs, exemptions, and configuration changes

All data stays in your AWS accounts. Refine connects to each account independently using read-only S3 access.

---

2. Prerequisites

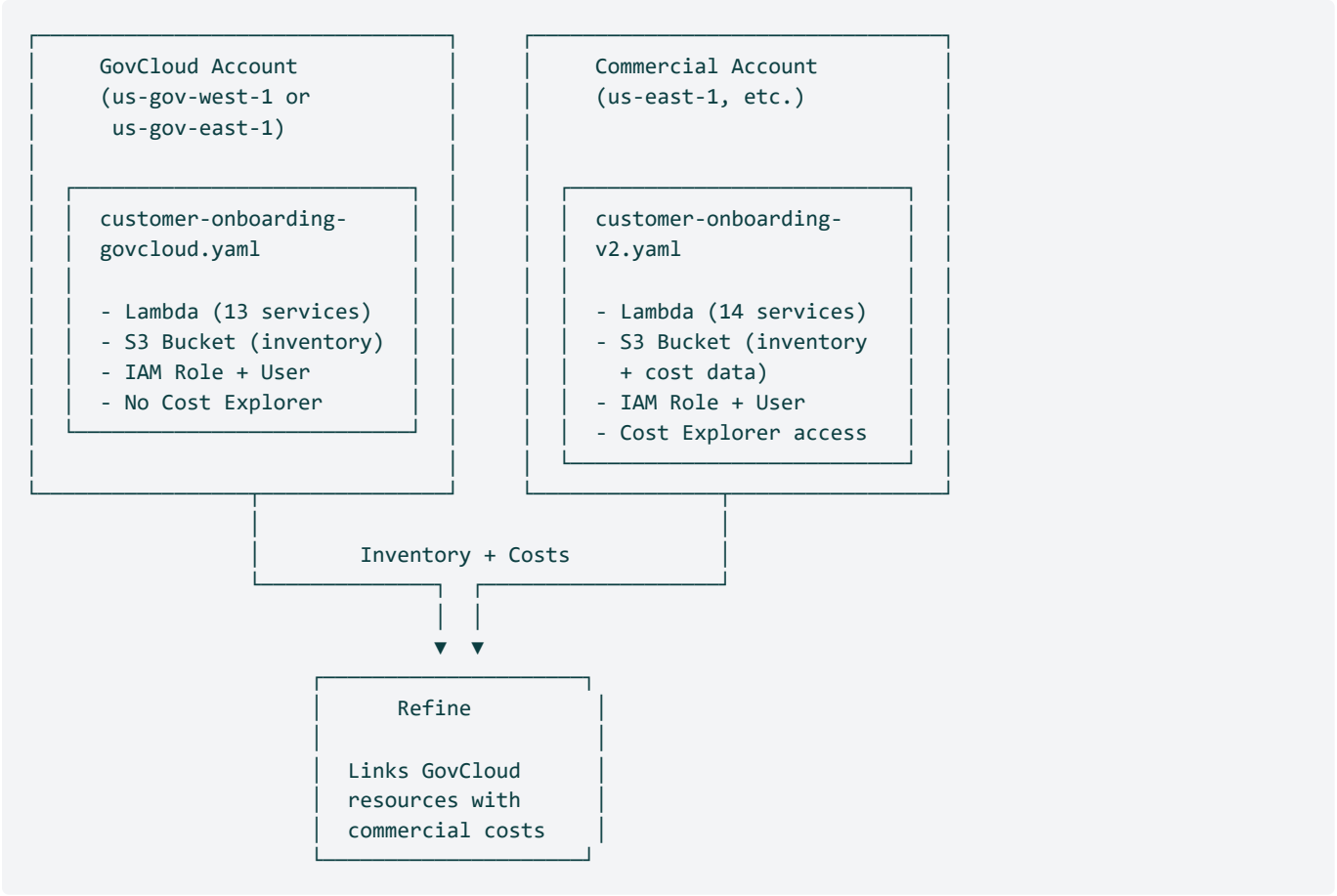
Before starting, ensure you have the following:

Requirement	Details
GovCloud AWS account	An active AWS GovCloud (US) account with resources to monitor
Linked commercial AWS account	The standard AWS account linked to your GovCloud account (where billing/Cost Explorer lives)
Both account IDs	12-digit account IDs for both the GovCloud and commercial accounts
Refine license	A valid `refine.license` with both account IDs authorized
Refine installed	A working Refine instance (see the Air-Gapped Setup Guide or Commercial Setup Guide)
AWS Console access	Admin-level access to both AWS accounts for deploying CloudFormation stacks

> ***License note:*** *Your Refine license must include both your GovCloud account ID and your commercial account ID. If your license only covers one account, contact Blacktip Solutions for an updated license before proceeding.*

---

3. Architecture



Key points:

- The GovCloud CF template (`customer-onboarding-govcloud.yaml`) collects **13 services** — everything except Cost Explorer, which is not available in GovCloud.
- The commercial CF template (`customer-onboarding-v2.yaml`) collects the full **14 services** including Cost Explorer data.
- Each account has its own IAM `RefineServiceUser` with access keys — there is no cross-partition role assumption.
- Refine reads from both S3 buckets independently and merges the data using the account link.

---

4. Step-by-Step Setup

Step 1 — Select "GovCloud + Linked Commercial"

In Refine, navigate to **AWS Accounts** in the sidebar. Click **Add Account**.

In the account type selector, choose **GovCloud + linked Commercial**. This tells Refine to expect a paired setup: one GovCloud account for inventory and one commercial account for cost data.

> *If you are adding GovCloud during initial onboarding (first-run Setup page), the same option appears in the account type dropdown.*

Step 2 — Enter GovCloud Account Details

Enter the following for your GovCloud account:

Field	Value
AWS Account ID	Your 12-digit GovCloud account ID
Region	`us-gov-west-1` or `us-gov-east-1`

> *GovCloud only has two regions. Select the region where the majority of your resources reside — this is where the CloudFormation stack will be deployed.*

Step 3 — Enter Linked Commercial Account Details

Enter the following for your linked commercial account:

Field	Value
AWS Account ID	Your 12-digit commercial account ID
Region	The region for your commercial CF stack (e.g., `us-east-1`)

> *This is the standard AWS account that is linked to your GovCloud account in AWS Organizations or through the GovCloud account creation process.*

Step 4 — Deploy GovCloud CloudFormation Template

Deploy the GovCloud-specific template in your GovCloud account:

1. Click **Download GovCloud Template** in Refine to get `customer-onboarding-govcloud.yaml`
2. Log into the **AWS GovCloud Console** (https://console.amazonaws-us-gov.com)
3. Navigate to **CloudFormation** → **Create Stack** → **Upload a template file**
4. Upload `customer-onboarding-govcloud.yaml`
5. Name the stack (e.g., `blacktip-refine-govcloud`)
6. Click through the configuration pages
7. Check the **IAM acknowledgment** checkbox → **Create stack**
8. Wait for **CREATE_COMPLETE** (~2-3 minutes)

> ***Important:*** *Deploy this template in a* ***GovCloud region*** *(`us-gov-west-1` or `us-gov-east-1`). Deploying it in a commercial region will fail.*

This stack collects inventory for **13 services**: EC2, RDS, EBS Snapshots, S3 Buckets, EBS Volumes, NAT Gateways, Load Balancers, Lambda, CloudWatch Logs, Fargate, ElastiCache, Batch Jobs, and Lightsail. Cost Explorer is excluded because it is not available in GovCloud.

Step 5 — Deploy Commercial CloudFormation Template

Deploy the standard template in your linked commercial account:

1. Click **Download Commercial Template** in Refine to get `customer-onboarding-v2.yaml`
2. Log into the **standard AWS Console** (https://console.aws.amazon.com)
3. Navigate to **CloudFormation** → **Create Stack** → **Upload a template file**
4. Upload `customer-onboarding-v2.yaml`
5. Name the stack (e.g., `blacktip-refine`)
6. Click through the configuration pages
7. Check the **IAM acknowledgment** checkbox → **Create stack**
8. Wait for **CREATE_COMPLETE** (~2-3 minutes)

This stack collects the full **14 services** including Cost Explorer. Cost data from this account is used for your GovCloud resources as well.

Step 6 — Copy CloudFormation Outputs into Refine

You need to copy outputs from **both** CloudFormation stacks into Refine.

GovCloud Account Outputs

From the GovCloud CloudFormation **Outputs** tab, copy these values into the GovCloud section in Refine:

CloudFormation Output	Refine Field
RoleArn	Role ARN
CostDataBucketName	S3 Bucket Name
(stack name you chose)	CloudFormation Stack Name
RefineServiceAccessKeyId	Access Key ID
RefineServiceSecretAccessKey	Secret Access Key

> ***Note:*** *The GovCloud `RoleArn` will start with `arn:aws-us-gov:iam::` instead of `arn:aws:iam::`. This is expected.*

Commercial Account Outputs

From the commercial CloudFormation **Outputs** tab, copy these values into the commercial section in Refine:

CloudFormation Output	Refine Field
RoleArn	Role ARN
CostDataBucketName	S3 Bucket Name
(stack name you chose)	CloudFormation Stack Name
RefineServiceAccessKeyId	Access Key ID
RefineServiceSecretAccessKey	Secret Access Key

> ***Secret Access Keys*** *are only shown once at stack creation time. If you miss one, you must delete the* `RefineServiceAccessKey` *resource (or the entire stack) and recreate it.*

Click **Save** after entering credentials for each account.

Step 7 — Validate Both Accounts

Click **Validate Setup** for each account. Refine tests:

- IAM role assumption using the provided credentials
- S3 bucket access for inventory data
- Cost Explorer access (commercial account only)

On success, both accounts show **Validated** status and an initial data sync triggers automatically.

> *If the GovCloud account validates but shows a warning about missing Cost Explorer data, this is expected. Cost data comes from the linked commercial account.*

---

5. What's Different in GovCloud

Understanding these differences helps avoid confusion during setup and day-to-day use.

No Cost Explorer API

GovCloud does not support the AWS Cost Explorer API. All cost data — including cost breakdowns, cost history, and Savings Plans/Reserved Instance information — comes from the linked commercial account.

In the Refine UI, cost columns for GovCloud resources are populated using data from the commercial account's Cost Explorer.

Only Two Regions

GovCloud has exactly two regions:

Region	Location
`us-gov-west-1`	AWS GovCloud (US-West) — Oregon
`us-gov-east-1`	AWS GovCloud (US-East) — Virginia

Refine scans both GovCloud regions regardless of which one you select for the CloudFormation stack.

ARN Format

GovCloud uses a different ARN partition:

```
Commercial:  arn:aws:iam::123456789012:role/RefineRole
GovCloud:    arn:aws-us-gov:iam::123456789012:role/RefineRole
```

Refine handles this automatically. You do not need to modify ARNs.

No Cross-Partition Role Assumption

AWS does not allow IAM role assumption across partitions (commercial ↔ GovCloud). This is why each account requires its own `RefineServiceUser` with access keys. Refine connects to each account independently using its own set of credentials.

Savings Plans and Reserved Instances

Savings Plans and Reserved Instances are managed and purchased in the **commercial account**. Refine reads this data from Cost Explorer in the commercial account and applies it to associated GovCloud resources where applicable.

---

6. Updating

Updating the Docker Image

Follow the update instructions in your primary setup guide (Air-Gapped or Commercial).

Updating CloudFormation Stacks

When a Refine update includes CloudFormation changes, you must update **both** stacks:

1. **GovCloud stack** — Download the latest `customer-onboarding-govcloud.yaml` from Refine and update the stack in the GovCloud Console
2. **Commercial stack** — Download the latest `customer-onboarding-v2.yaml` from Refine and update the stack in the standard AWS Console

For each stack:

1. Go to **CloudFormation** → select your Refine stack → **Update**
2. Choose **Replace current template** → upload the new template
3. Click through all pages — existing parameters are preserved automatically
4. Acknowledge the IAM capabilities checkbox → **Update stack**
5. Wait for **UPDATE_COMPLETE**

Do **not** delete and recreate stacks — updating preserves your S3 bucket and all collected data.

> *Refine alerts you when a stack update is needed. A **yellow banner** appears on the **AWS Accounts** page, and each account row shows an **"Update CF"** button when an update is available.*

---

7. Troubleshooting

Problem	Solution
"CF version could not be read"	Stack name mismatch — Refine auto-detects the stack name from the Role ARN. Ensure the CloudFormation Stack Name field in Refine matches the actual stack name in AWS
"InvalidClientTokenId"	Access key was rotated or deleted. Go to CloudFormation → Outputs and get the current `RefineServiceAccessKeyId` and `RefineServiceSecretAccessKey`. If the key was manually deleted, recreate the stack
"No Cost Explorer data" for GovCloud	This is expected. Cost Explorer is not available in GovCloud. Ensure your linked commercial account is validated and syncing — cost data comes from there
Region mismatch error	Ensure the GovCloud CF template was deployed in a `us-gov-*` region, not a commercial region. The commercial template should be deployed in a standard region (e.g., `us-east-1`)
GovCloud CF template fails to deploy	Check that you are logged into the GovCloud Console (console.amazonaws-us-gov.com), not the standard Console. Verify IAM permissions allow CloudFormation stack creation
Resources missing from GovCloud	Verify the Lambda function is running in GovCloud. Check CloudWatch Logs in the GovCloud Console for the Refine Lambda. Click **Sync Now** in Refine
Cost data not associating with GovCloud resources	Verify both accounts are validated and linked. The commercial account must have Cost Explorer enabled (activated in the AWS Billing Console)

Checking Logs

```
# Refine application logs
docker compose logs --tail 100

# Filter for GovCloud-related messages
docker compose logs --tail 100 | grep -i govcloud
```

---

8. FAQ

Can I have resources in both accounts?

Yes. Both the GovCloud account and the commercial account are independently monitored. Refine collects inventory from each account separately. Resources in the commercial account appear alongside their own cost data. Resources in GovCloud appear with cost data sourced from the linked commercial account.

How are recommendations linked across accounts?

Cost data from the commercial account's Cost Explorer is associated with GovCloud resources through the account link you configured in Refine. When Refine generates recommendations (e.g., right-sizing an EC2 instance in GovCloud), it uses cost data from the commercial account to calculate potential savings.

Do I need separate AWS credentials for each account?

Yes. Each account has its own `RefineServiceUser` created by its CloudFormation stack, with its own Access Key ID and Secret Access Key. There is no credential sharing between the GovCloud and commercial accounts because AWS does not allow cross-partition role assumption.

Can I add multiple GovCloud accounts?

Yes. Each GovCloud account needs its own linked commercial account. Repeat the setup process (Steps 1-7) for each pair.

What if my GovCloud account and commercial account are not linked?

The GovCloud account must be linked to a commercial account through AWS. This link is established when the GovCloud account is created — it cannot be added after the fact. If your accounts are not linked, cost data will not be associated with GovCloud resources. Contact your AWS account manager for assistance.

Do I need to deploy in both GovCloud regions?

No. Deploy the CloudFormation stack in one GovCloud region. The Refine Lambda scans resources in **both** `us-gov-west-1` and `us-gov-east-1` regardless of where the stack is deployed.

Is data transmitted between GovCloud and commercial partitions?

No. Refine reads from each account independently using separate credentials and separate S3 buckets. The association between GovCloud resources and commercial cost data happens entirely within your Refine instance — no data crosses the AWS partition boundary.

Need Help?

Contact Blacktip Solutions at **support@blacktipsolutions.com**
