Refine — Azure Setup Guide

Onboard an Azure subscription to Refine for cost-optimization recommendations.

Two paths to provision everything Refine needs — **pick one**:

1. **Cloud Shell one-liner (recommended)** — paste a single `curl | bash` into Azure Cloud Shell and it runs end-to-end (~60 s): app registration → service principal → reader role → storage account → cost-management export. Prints the values you paste into the Refine UI.
2. **Bicep template (GitOps-friendly)** — `infra/azure/refine-onboarding.bicep` deploys the same resources but requires ~4 follow-up `az` commands for the app registration / client secret (Bicep can't create them).

Refine itself runs in your own environment (laptop, EC2, on-prem, or Azure VM) and reads this data over HTTPS to `management.azure.com` (or the USGov / China endpoint). Nothing about your data crosses to Blacktip — Refine reads straight from your storage account.

What gets deployed

Resource	Purpose
Entra ID App Registration + Service Principal	Refine authenticates as this
Reader role assigned at subscription scope	Read-only access to Resource Graph + Monitor metrics
Storage Account + Blob Container (`refine-cost-export`)	Destination for daily Cost Management Export drops
Daily Cost Management Export	Auto-configured by the Cloud Shell script

---

Network requirements

Refine's host must reach Microsoft's Azure endpoints over HTTPS:

- **Commercial:** `login.microsoftonline.com` + `management.azure.com` + `<storage>.blob.core.windows.net`
- **USGov:** `login.microsoftonline.us` + `management.usgovcloudapi.net` + `<storage>.blob.core.usgovcloudapi.net`
- **China:** `login.partner.microsoftonline.cn` + `management.chinacloudapi.cn` + `<storage>.blob.core.chinacloudapi.cn`

Azure has no private-link alternative for Cost Management. **Air-gapped deployments cannot use Azure cost monitoring**; use Resource Graph inventory only or stick with AWS for air-gapped installs.

Azure Government & sovereign clouds (auto-detected)

The onboarding script **auto-detects which Azure cloud you're in** via `az cloud show` and configures the correct endpoints + region automatically:

Cloud	Environment value	ARM endpoint used	Default region
Azure Commercial	`Public`	management.azure.com	eastus
Azure US Government	`USGov`	management.usgovcloudapi.net	usgovvirginia
Azure China	`China`	management.chinacloudapi.cn	chinaeast2
Azure Germany	`German`	management.microsoftazure.de	germanycentral

For **US Government** subscriptions: run the script from a Gov Cloud Shell (`portal.azure.us`) and it picks `USGov` automatically — it prompts you to confirm the region (you can pick `usgovvirginia` / `usgovtexas` / `usgovarizona` / `usgoviowa` , or set `RG_LOCATION=...` to skip the prompt). The resulting **Azure Environment** value the script prints is what you select in the Refine Add-Account modal so the SDK talks to the right cloud.

There is no separate "Gov SKU" — every Refine install can connect Gov and Commercial subscriptions side by side.

Path A — Cloud Shell one-liner (recommended)

1. Open **Azure Cloud Shell** at https://shell.azure.com in the tenant you want to monitor. Select **Bash** mode.
2. Make sure the right subscription is active:

   ```
   az account set --subscription <your-subscription-id>
   ```

3. Paste the script:

   ```
   # If your repo is public:
   curl -sL https://raw.githubusercontent.com/eichenbergerb/Blacktip_Refine/main/infra/azure/refine-onboa

   # OR (if private): upload infra/azure/refine-onboarding.sh from your delivery
   # ZIP via Cloud Shell's "Manage files → Upload" then run:
   chmod +x refine-onboarding.sh && ./refine-onboarding.sh
   ```

4. Confirm `y` at the prompt. The script prints the values you paste into Refine:
   - **Azure Subscription ID**
   - **Azure Tenant ID**
   - **Azure Client ID** (App Registration)
   - **Azure Client Secret** ← copy this NOW; Azure never shows it again
   - **Azure Environment** (`Public` / `USGov` / `China` — reflects the cloud the script detected)
   - **Storage Account** (e.g. `refinecost4b0c5c55`)
   - **Storage Container** (`refine-cost-export`)
5. In Refine, click **Cloud Accounts** → **Add Account** → **Azure** and paste those seven values. Click **Add** — validation runs automatically.

If Cost Management Export creation fails (Pay-As-You-Go subscriptions need EA / MCA to enable Cost Management), the script still completes. Inventory sync runs without cost data; you can configure the export manually later in the Portal under Cost Management + Billing → Export.

Path B — Bicep template (manual)

```
az cloud set --name AzureCloud           # or AzureUSGovernment / AzureChinaCloud
az login
az account set --subscription <your-subscription-id>

# Deploy at subscription scope
az deployment sub create \
  --location eastus \
  --template-file infra/azure/refine-onboarding.bicep \
  --parameters customerEmail='ops@yourco.com' externalId='<paste-from-refine-ui>'

# Create the App Registration + Service Principal (Bicep can't do this)
az ad app create --display-name "Refine for Cost Management"
APP_ID=$(az ad app list --display-name "Refine for Cost Management" --query "[0].appId" -o tsv)
az ad sp create --id $APP_ID
ROLE_ID=$(az deployment sub show --name refine-onboarding --query "properties.outputs.customRoleId.value"
az role assignment create --assignee $APP_ID --role $ROLE_ID --scope /subscriptions/$(az account show --qu

# Generate a client secret
az ad app credential reset --id $APP_ID --years 1
# → copy the `password` field — that's your client secret
```

Then paste credentials into Refine the same way as Path A.

Day-2 hardening

After the first successful sync:

1. Rotate the App Registration client secret every 90 days:

   ```
   az ad app credential reset --id $APP_ID --years 1
   ```

2. Update the secret in Refine: **Cloud Accounts** → **Blacktip-Azure** → **Edit**
3. The original secret is now invalidated.

Supported Azure resources (v2.27)

Refine generates recommendations for:

- **Azure VMs** (rightsizing + idle detection with 1mo / 3mo / 1yr period metrics)
- **Managed Disks** (orphaned + over-provisioned premium-tier downgrade)
- **Storage Accounts / Blob containers** (lifecycle policy + access-tier moves)
- **Azure SQL Database** (rightsizing DTU/vCore + reserved capacity)
- **Public IPs** (orphaned static IPs)
- **AKS** (node-pool rightsizing + idle node detection)
- **Azure Functions** (memory tuning + invocation/error/throttle history)

Period metrics (CPU / memory / network avg + peak across 1 mo / 3 mo / 1 yr) land in the DB via the Azure Monitor metrics collector that runs each nightly sync. Cost data lands once the daily Cost Management Export has dropped its first CSV (≤ 6 h for the first drop after configuration).

Troubleshooting

Problem	Fix
Cloud Shell `404` from `curl`	Repo is private — upload `infra/azure/refine-onboarding.sh` from your delivery ZIP via Cloud Shell's **Manage files** → **Upload** instead.
"AAD authentication failed" on validate	Re-check tenant_id, client_id, client_secret. Confirm you're on the right Azure cloud (Public / USGov / China).
Validation passes but no resources show up	Click **Sync Now** in the UI. Inventory sync runs as a background task — give it 30–60 s, then refresh.
No cost data after 24 h	Cost Management Export takes up to 6 h for the first drop. Check the storage container has a recent `.csv` / `.csv.gz`.
"Permission denied on Microsoft.CostManagement/exports/read"	The Reader role assignment didn't propagate yet. Wait 60 s and re-validate, or re-run the script.
Resources visible in inventory but no period metrics (avg/peak shows "—")	Azure Monitor metrics collect on the nightly sync. They appear after the first sync completes, ~10 minutes after Add.

Need help?

Email **support@blacktipsolutions.com**.
