Egress and Ingress solution

Egress/Ingress

Network connections involve senders and receivers, with messages potentially taking different paths in each direction (asymmetric routing). Since ingress for one side is egress for the other, proper IP management is essential.

Exalate Cloud provides dedicated endpoints for **ingress** (inbound) and **egress** (outbound) traffic to simplify IP management:

Ingress IPs (`ingress.exalate.cloud`)

Use these IPs when sending requests to Exalate (e.g., via Exalate APIs).

Command to retrieve Ingress IPs with regions:

```
for ip in $(dig +short ingress.exalate.cloud); do
    echo "IP: $ip | Region: $(curl -s https://ipinfo.io/$ip | jq -r '.region')"
done
```

Egress IPs (`egress.exalate.cloud`)

Whitelist these IPs to allow outbound connections from Exalate (e.g., for Exalate-initiated API calls).

Command to retrieve Egress IPs with regions:

```
for ip in $(dig +short egress.exalate.cloud); do
    echo "IP: $ip | Region: $(curl -s https://ipinfo.io/$ip | jq -r '.region')"
done
```

Notes:

- These commands require `dig` , `curl` , and `jq` . On Windows, use WSL or Git Bash.

- For security, restrict whitelisted IPs to only necessary regions.

- More IPs may be added in the future so if your solution requires so you may recheck the available ones and change accordingly.

YouTube Channel ⧉

Ebooks ⧉

Still need help?

Join our Community ⧉

Visit our Service Desk ⧉

Find a Partner ⧉