GCC 2.0 Tech Talks

- AWS GA is targeted at **4th May 2022**.
- If and when we talk about Native Services, we will probably cite **AWS only** as these are gearing towards AWS GA preparation.
- Information on Azure will be shared in coming months (to recap, Azure GA will be by Q3 2022).
- All slides will be shared and most of the documentation will also be translated to either Developers Portal (accessible by everyone) or Docs Portal (only accessible by for TechPass account holders).
- All the slides can be shared with existing contractors who are required to manage Projects on GCC as deemed fit by Agencies.
- The series of "Brown Bag" lunch time tech talk is arranged so as to ensure more people can join us in view that some will clash with your meetings. Please feel free to have your lunch while you join us.

For Your Info

- You will be put on mute by default.
- Video should be turned off.

Q&A Segment

- Type in message box when you want to ask a question.
- Wait to be acknowledged by the presenter before speaking.
- Unmute your microphone and state your name and agency clearly.

Session Recording

- Please note that the series of GCC 2.0 Tech Talks will be recorded.
- The video recordings will be made available (in SharePoint).

Let Us Know Your Feedback!

https://form.gov.sg/625cbc85b91a650012696081

- Let us know what went well and how we can improve.
- We want to ensure that we are bringing the right contents to you so as to help Agencies.
- If you have any questions, please reach out to us at Ask_CODEX@tech.gov.sg

Deep diving GCC 2.0 Common Service

Andrew Nai
GDS / ENP - Cloud

Date: 28 April 2022

TABLE OF CONTENTS

1. Background
2. Overview
   a. GCC PIM
   b. GCC EDR
   c. GCC SM
3. Requirements for new GCC 2.0 tenants to onboard GCC CS
4. Requirements for migrated GCC 1.0 tenants to GCC 2.0 to onboard or continuation with GCC CS
5. Past ICT Briefing on GCC CS
6. Q&A

Background

- GCC Common Services (CS)* is a suite of IM8 mandated services offered in GCC for Agencies to subscribe.
- GCC CS assists Agencies to speed up their cloud adoption journey by leveraging on these centrally managed services.
- GCC CS was operationalized in Nov 2021 and comprises of the following three key services:

#	GCC Common Services	Policy	Clauses
1	GCC Privileged Identity Management (PIM)	APPLICATION DEVELOPMENT SECURITY	**Clause 2.4/S1 and 2.4/G1.** Agencies shall manage and track the use of privileged accounts, including interactive and service accounts, by implementing the following security controls: a) **Privileged Identity Management (PIM)** tools to manage privileged interactive accounts; and b) **PIM** or **Secrets Management tools** with secret rotation capability to manage service accounts.
2	Endpoint Detection & Response (EDR)	ICT & SS Management Role & System-based Views	**Clause 7.2/S5**. Agencies shall implement **Endpoint Detection and Response (EDR) tools** to protect their systems from advanced threats.
3	Secret Management (SM)	APPLICATION DEVELOPMENT SECURITY	**Clause 2.2/S4**. Agencies shall encrypt and store authentication credentials and secret keys that are used in program codes such as automation scripts, mobile and web applications, inside secure protected storages; Agencies can either use secure protected storage methods that are recommended as best practices by the programming language/framework providers or runtime/hosting platforms, or use secure protected storage that are available in **secret management** tools

* Refer to this link GCC CS Product Page to understand more on offerings, benefits, onboarding steps and pricing.

Overview of GCC Common Services*

GCC CS	Product Overview	Key Features
GCC PIM	**GCC Privileged Identity Management (PIM)** offers Agencies a centrally managed privileged identity management solution to enable tracking, account elevation approval and session recording on privileged account access and usage on Agencies' systems hosted in GCC.	**Reduce Risk of Unauthorised Use of Privilege Accounts** GCC PIM provides Agencies with the ability to manage access control, granting of, usage, tracking and logging of interactive privileged accounts to its administrators. It removes the individual administrators from holding on to privileged accounts and limits access to only when there is a business need and approvals are obtained. GCC PIM supports workflow for credential access approval, session recording and proactively detects suspicious behavior to ensure that privileged accounts such as administrator, root or super user, held by individuals are closely monitored for non-business related activities or unauthorized changes.
GCC EDR	**GCC Endpoint Detection & Response (EDR)** offers Agencies a centrally managed cybersecurity solution to enable timely detection and investigation of potential IT security events on Agencies' systems.	**Reduce Risk of Systems Being Compromised, Leading to Data Breaches** GCC EDR provides visibility and insights for discovery, investigation and response to advanced file-less malware threats spreading across multiple endpoints using behavior-based anomaly detection and signature based matching technologies. Security teams can then perform preventive threat hunting across multiple endpoints to quickly zoom in, record suspicious activities and isolate malicious binaries or executables in compromised workloads from lateral spread and data breaches
GCC SM	**GCC Secret Management (SM)** offers Agencies a solution to protect their secrets each time an application requests for programmatic access.	**Reduce Risk of Secret Leakage** GCC SM eliminates the risk of permanent secrets embedded in codes and published to public repositories by issuing short lived secrets to authorised applications. This reduces the risk of permanent secrets being leaked and misused by non-authorised parties that actively hunt public code repositories.

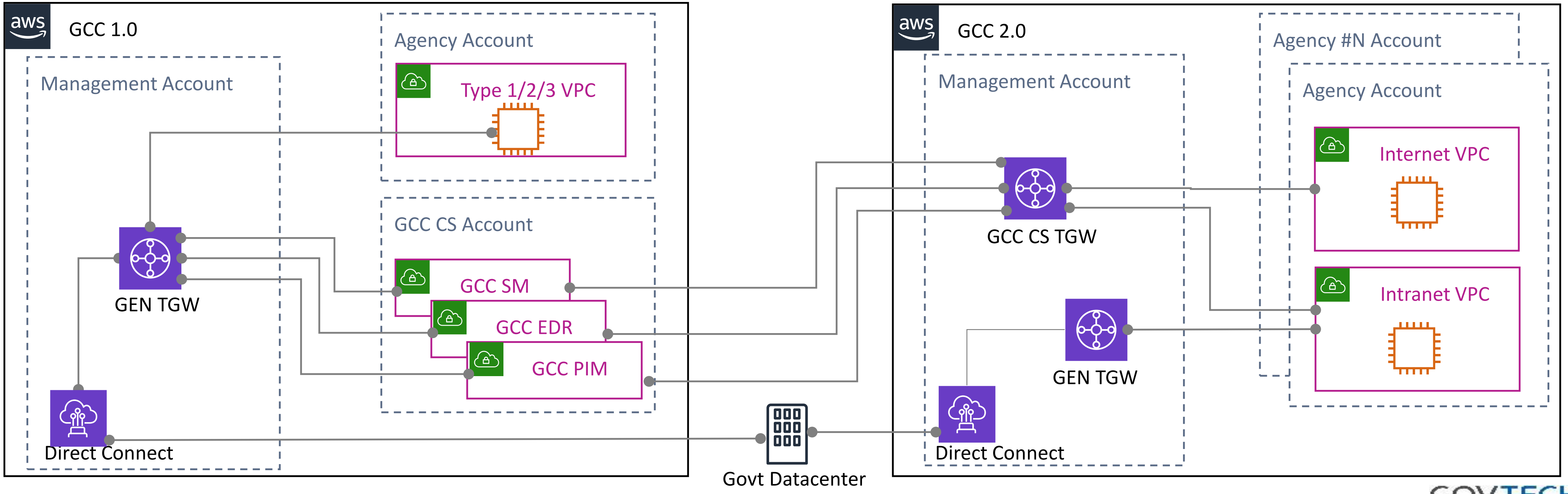
* Refer to this link GCC CS Product Page to understand more on offerings, benefits, onboarding steps and pricing.

GCC CS connectivity to new compartments in GCC 2.0

- A new GCC CS Transit Gateway (TGW) is setup centrally in GCC 2.0.

- At GCC 2.0 GA, only the following new compartments can onboard to GCC CS:
  - Intranet Compartment
  - Internet Compartment

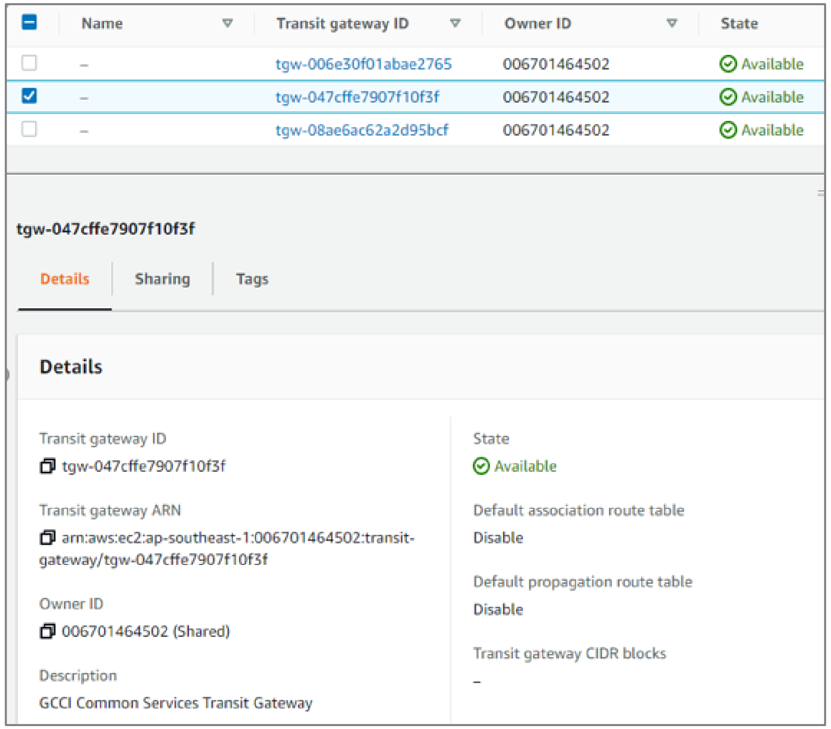
- The support for Agency Managed Compartment to onboard GCC CS will be shared after GCC 2.0 GA.



New GCC 2.0 tenants to onboard GCC CS (1/3)

Agency with workloads in GCC 2.0 who wishes to onboard GCC CS to comply with policies are required to:

Step	Instructions
1	Pre-requisites: a. Login to AWS console from GCC 2.0 CMP b. Under VPC*, click on Transit Gateway. c. Validate the GCC CS TGW is provisioned by inspecting the details (see Figure 1) d. Validate transit gateway attachment is attached to the VPC (see Figure 2). e. Complete the GCC CS onboarding steps (link)



▬	Name	Transit gateway ID	Owner ID	State
□	–	tgw-006e30f01abae2765	006701464502	✓ Available
☑	–	tgw-047cffe7907f10f3f	006701464502	✓ Available
□	–	tgw-08ae6ac62a2d95bcf	006701464502	✓ Available

tgw-047cffe7907f10f3f

Details

Transit gateway ID
tgw-047cffe7907f10f3f

Transit gateway ARN
arn:aws:ec2:ap-southeast-1:006701464502:transit-gateway/tgw-047cffe7907f10f3f

Owner ID
006701464502 (Shared)

Description
GCCI Common Services Transit Gateway

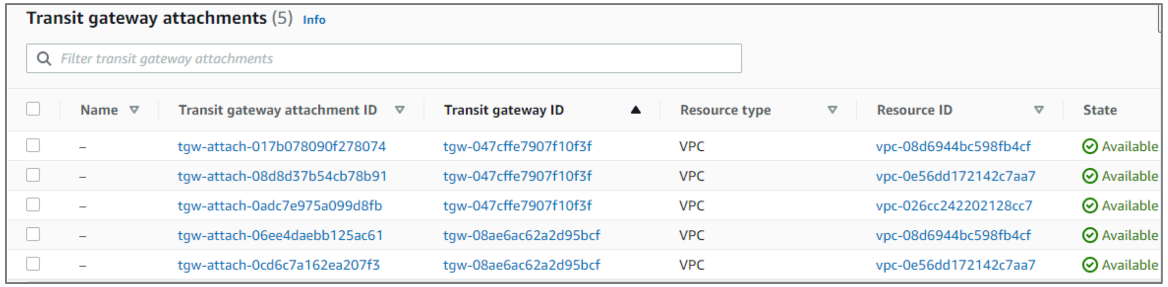
State
✓ Available

Default association route table
Disable

Default propagation route table
Disable

Transit gateway CIDR blocks
–

Figure 1



Transit gateway attachments (5) Info

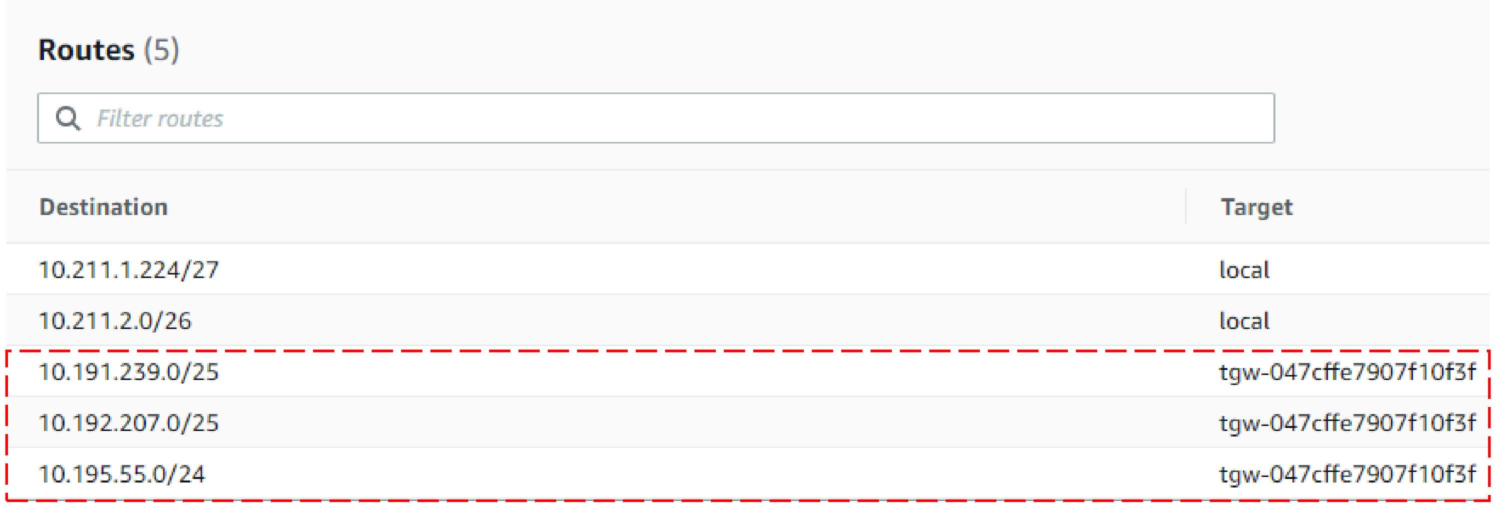
□	Name	Transit gateway attachment ID	Transit gateway ID	Resource type	Resource ID	State
□	–	tgw-attach-017b078090f278074	tgw-047cffe7907f10f3f	VPC	vpc-08d6944bc598fb4cf	✓ Available
□	–	tgw-attach-08d8d37b54cb78b91	tgw-047cffe7907f10f3f	VPC	vpc-0e56dd172142c7aa7	✓ Available
□	–	tgw-attach-0adc7e975a099d8fb	tgw-047cffe7907f10f3f	VPC	vpc-026cc242202128cc7	✓ Available
□	–	tgw-attach-06ee4daebb125ac61	tgw-08ae6ac62a2d95bcf	VPC	vpc-08d6944bc598fb4cf	✓ Available
□	–	tgw-attach-0cd6c7a162ea207f3	tgw-08ae6ac62a2d95bcf	VPC	vpc-0e56dd172142c7aa7	✓ Available

Figure 2

* Only applicable to intranet and internet compartments at GA

New GCC 2.0 tenants to onboard GCC CS (2/3)

Step	Instructions
2	a. Under the newly created intranet or internet VPC, click to edit the main route table. b. Add the respective CIDR of GCC CS services (10.191.230/25, 10.192.207.0/25 and 10.195.55.0/24) to destination and GCC CS TGW to Target and click save. c. The main route table should have both local and GCC CS TGW after completion (see Figure 3)



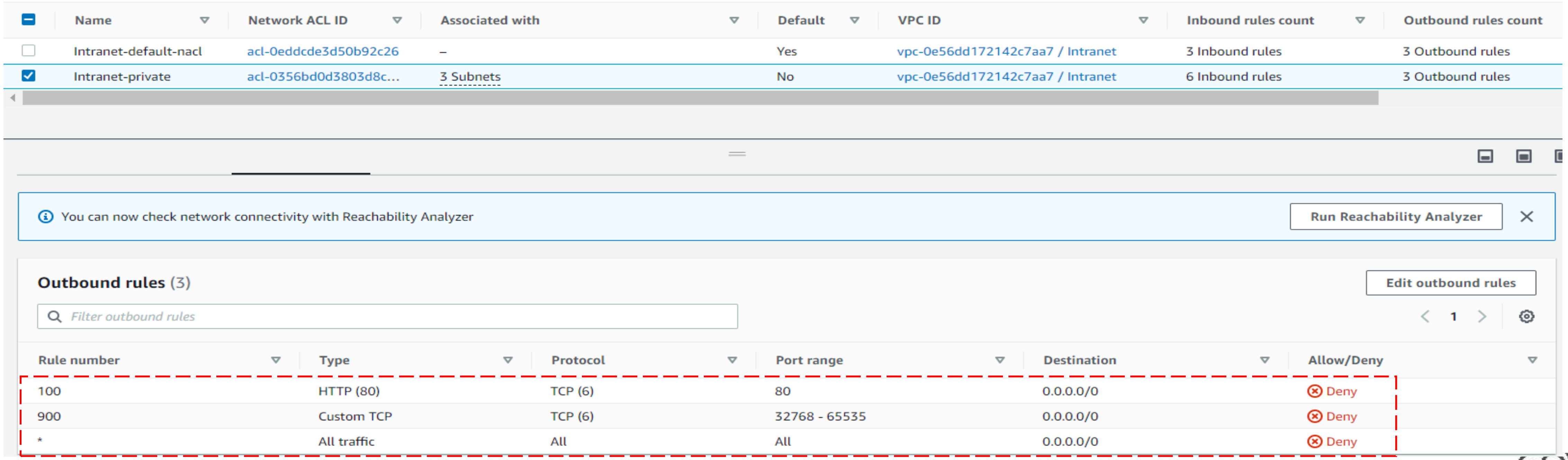
Routes (5)

Destination	Target
10.211.1.224/27	local
10.211.2.0/26	local
10.191.239.0/25	tgw-047cffe7907f10f3f
10.192.207.0/25	tgw-047cffe7907f10f3f
10.195.55.0/24	tgw-047cffe7907f10f3f

Figure 3

New GCC 2.0 tenants to onboard GCC CS (3/3)

Step	Instructions
3	a. Under VPC, the non default nacl is configure to deny all outbound traffic to ensure least privilege of access (see Figure 4) b. Agency are to require to edit and to allow the protocol and ports required per GCC CS onboarding guide.
4	a. Under VPC, configure security group to allow protocol and ports required per GCC CS onboarding guide.



☐	Name	Network ACL ID	Associated with	Default	VPC ID	Inbound rules count	Outbound rules count
☐	Intranet-default-nacl	acl-0eddcde3d50b92c26	–	Yes	vpc-0e56dd172142c7aa7 / Intranet	3 Inbound rules	3 Outbound rules
☑	Intranet-private	acl-0356bd0d3803d8c...	3 Subnets	No	vpc-0e56dd172142c7aa7 / Intranet	6 Inbound rules	3 Outbound rules

You can now check network connectivity with Reachability Analyzer

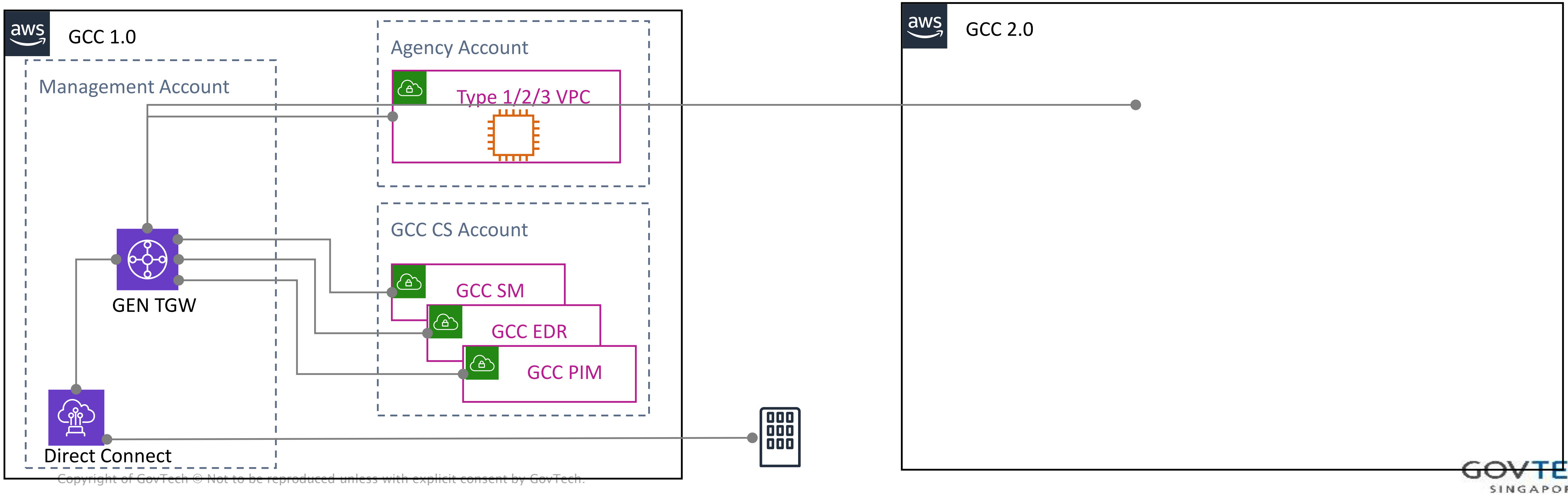
Outbound rules (3)

Rule number	Type	Protocol	Port range	Destination	Allow/Deny
100	HTTP (80)	TCP (6)	80	0.0.0.0/0	⊗ Deny
900	Custom TCP	TCP (6)	32768 - 65535	0.0.0.0/0	⊗ Deny
*	All traffic	All	All	0.0.0.0/0	⊗ Deny

Figure 4

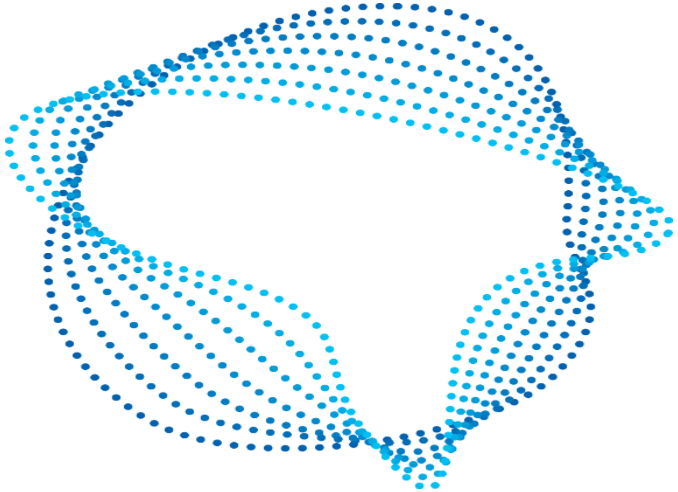
Migrated GCC 1.0 tenants to GCC 2.0 to use/onboard GCC CS

- Currently, Agencies in GCC 1.0 who are existing tenants in GCC CS uses GEN TGW in GCC 1.0 to consumer GCC CS.
- When Agency migrates their accounts from GCC 1.0 to 2.0, their migrated VPCs will continue to connect to GCC CS via GCC 1.0 GEN TGW.
- Likewise, migrated VPCs in GCC 2.0 who wishes to onboard GCC CS will be connected via GCC 1.0 GEN TGW.



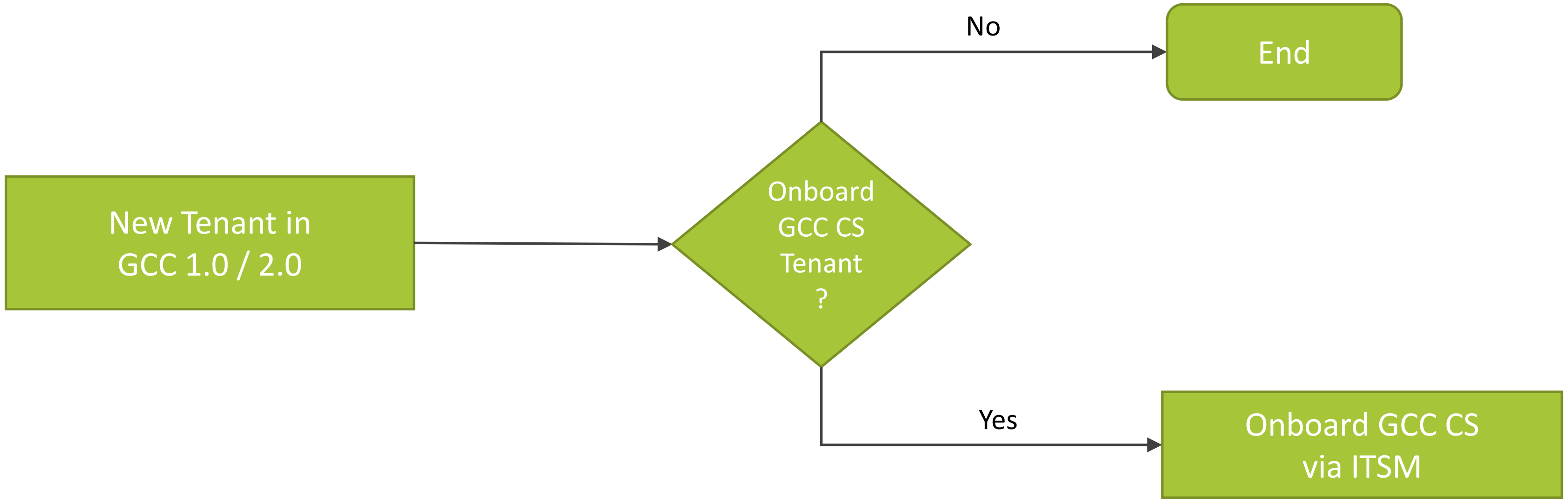
Past ICT Briefing sharing on GCC CS

#	ICT Briefing #	ICT Topic and link	Date
1	76.1h	GCC Common Services – Secret Management	12 Feb 2020
2	77.1k	GCC Common Services Updates	11 Mar 2020
3	95	GCC Common Services Updates	13 Oct 2021
4	96.1	Agency-Managed TGW	10 Nov 2021
5	96.1	GCC Common Services (CS) Billing Workflow	10 Nov 2021
6	97.1	GCC Common Services (CS) Billing	12 Jan 2022



Q&A

New Tenant in GCC 1.0 or 2.0 who needs to onboard GCC CS



- This scenario applies to both new tenant onboarding to GCC 1.0 and 2.0 which are issued with unique tenant ID.
- GCC CS charges by <u>**Tenant ID (i.e. CMP ID)**</u>
- Agency who needs GCC CS for their project needs can onboard via ITSM.

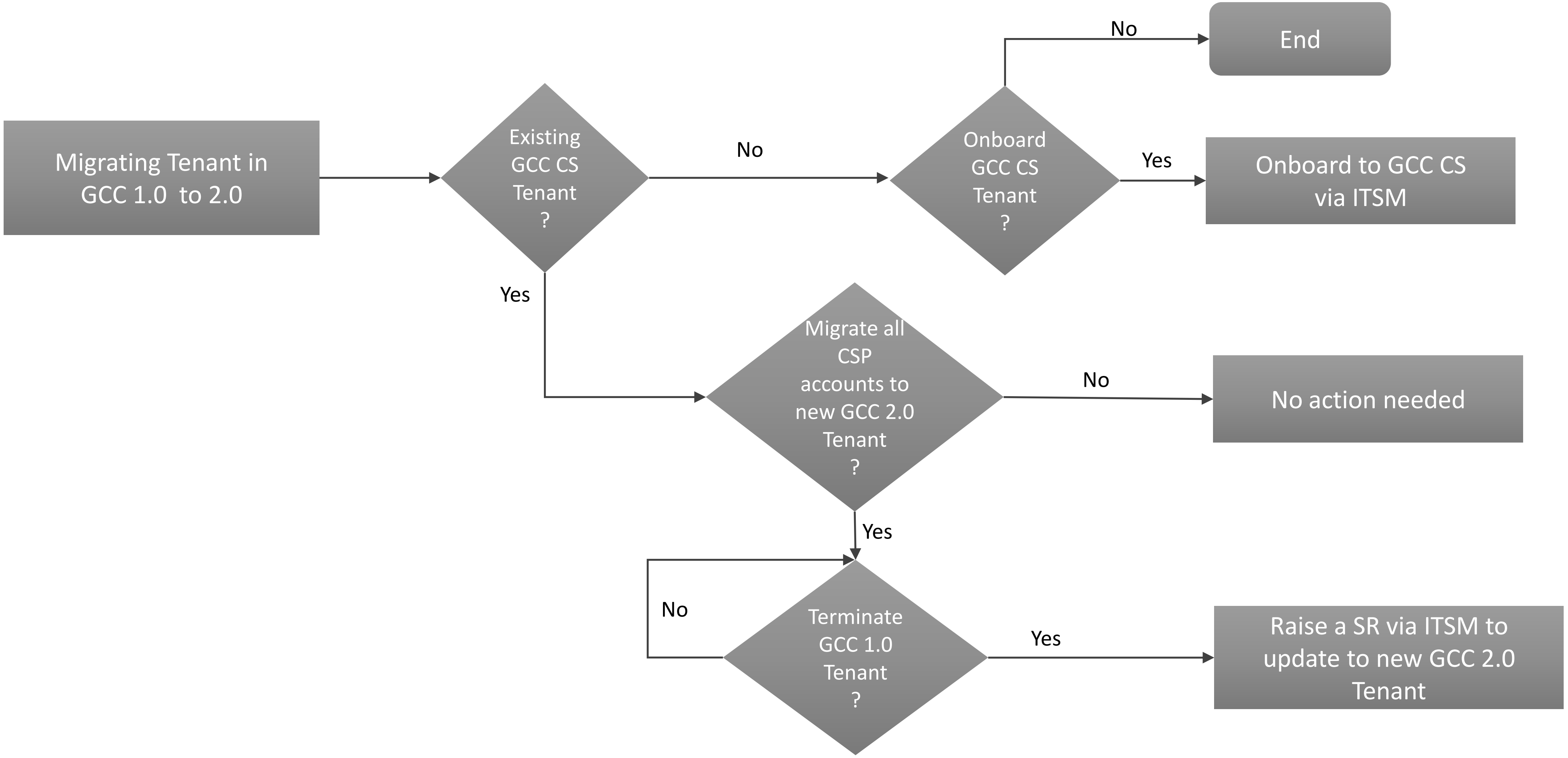
RESTRICTED – Do not forward/distribute. For Internal Government Use Only.

Frequently Asked Questions (1/5)

Q1	I am a new Agency freshly onboard to GCC 2.0 and I do not have any prior GCC 1.0 tenant account, how do I onboard to GCC CS?
A1	• Agency who is not a prior GCC 1.0 tenant and has onboard straight into GCC 2.0 tenant may onboard to GCC CS by following the instructions in GCC CS Product Page to understand more on offerings, benefits, onboarding steps and pricing.

Q2	I am a existing Agency onboard to GCC 1.0. Are there any changes to GCC CS services to my existing GCC 1.0 tenant account, CSP accounts and workloads in GCC 1.0?
A2	• There are no changes to existing GCC 1.0 tenants.

Migrating GCC 1.0 Tenant to GCC 2.0 & GCC CS



Migrating Tenant in GCC 1.0 to 2.0

Existing GCC CS Tenant ?

No

Onboard GCC CS Tenant ?

No

End

Yes

Onboard to GCC CS via ITSM

Yes

Migrate all CSP accounts to new GCC 2.0 Tenant ?

No

No action needed

Yes

Terminate GCC 1.0 Tenant ?

No

Yes

Raise a SR via ITSM to update to new GCC 2.0 Tenant

RESTRICTED – Do not forward/distribute. For Internal Government Use Only.

9 Feb 2022

Frequently Asked Questions (2/5)

^ GCC CS Product Page

Q3	- I am a existing Agency onboard in GCC 1.0 and GCC CS. - I have onboarded to GCC 2.0 and create a new tenant ID for new project. - I intent to onboard GCC CS for the workloads in this new project. - What are the changes on GCC CS services and billing to my Agency?
A3	- GCC 1.0 and 2.0 maintains separate and different tenant IDs. - GCC CS tenant ID is provision based on either GCC 1.0 or 2.0 tenant ID^. - Agency may onboard the new GCC 2.0 tenant ID to GCC CS by following the instructions in GCC CS Product Page to understand more on offerings, benefits, onboarding steps and pricing. - GCC CS will invoice the Agency based on GCC Tenant ID(s) onboard to GCC CS.

Frequently Asked Questions (3/5)

^ GCC CS Product Page

Q4	• I am a existing Agency onboard in GCC 1.0 and GCC CS. • I have onboarded to GCC 2.0 and **fully migrated** all of my CSP accounts and workloads under this GCC 1.0 tenant ID to the new tenant ID in GCC 2.0. • I intent to decommission the GCC 1.0 tenant ID. • What are the changes on GCC CS services and billing to my Agency?
A4	• GCC 1.0 and 2.0 maintains separate and different tenant IDs. • GCC CS tenant ID is provision based on either GCC 1.0 or 2.0 tenant ID^. • GCC CS will continue to invoice the Agency based on GCC 1.0 tenant ID onboard to GCC CS. • Agency shall raise a GCC CS Service Request in ITSM to update to the new GCC 2.0 tenant ID **prior to the termination of GCC 1.0 tenant ID**. This is to ensure continuity in CS services offering and billing.

Frequently Asked Questions (4/5)

^ GCC CS Product Page

Q5	• I am a existing Agency onboard in GCC 1.0 and GCC CS with **one tenant ID**. • I have onboarded to GCC 2.0 and **migrate some of my CSP accounts and workloads** under this GCC 1.0 tenant ID to a new tenant ID in GCC 2.0. • I intent to decommission the GCC 1.0 tenant ID after all my CSP accounts and workloads are migrated to the GCC 2.0 tenant ID in the future. • What are the changes on GCC CS services and billing to my Agency?
A5	• GCC 1.0 and 2.0 maintains separate and different tenant IDs. • GCC CS tenant ID is provision based on either GCC 1.0 or 2.0 tenant ID^. • GCC CS will continue to invoice the Agency based on onboard GCC tenant id to GCC CS. • Agency shall raise a GCC CS Service Request in ITSM to update to the new GCC 2.0 tenant ID **prior to the termination of GCC 1.0 tenant ID**. This is to ensure continuity in CS services offering and billing.

Frequently Asked Questions (5/5)

^ GCC CS Product Page

Q6	• I am a existing Agency onboard to GCC 1.0 and GCC CS with **multiple tenant IDs** (i.e. One tenant ID to one project) • I have onboarded to GCC 2.0 and **migrate one of my GCC 1.0 tenant ID** to a new tenant ID in GCC 2.0 for one of my project. • I intent to decommission the GCC 1.0 tenant ID after migration completion. • What are the changes on GCC CS services and billing to my Agency?
A6	• GCC 1.0 and 2.0 maintains separate and different tenant IDs. • GCC CS tenant ID is provision based on either GCC 1.0 or 2.0 tenant ID^. • GCC CS will continue to invoices Agency based on existing GCC 1.0 tenant ID onboard to GCC CS. • Agency shall raise a GCC CS Service Request in ITSM to update to the new GCC 2.0 tenant ID **prior to the termination of GCC 1.0 tenant ID**. This is to ensure continuity in CS services offering and billing.

THANK YOU

Questions and Answers

We Want to Hear Your Feedback!

https://form.gov.sg/625cbc85b91a650012696081

- Let us know what went well and how we can improve.
- We want to ensure that we are bringing the right contents to you so as to help Agencies.
- If you have any questions, please reach out to us at Ask_CODEX@tech.gov.sg