

TELSTRA CLOUD
INFRASTRUCTURE
UPLIFT
USER GUIDE



WELCOME TO THE TELSTRA CLOUD INFRASTRUCTURE UPLIFT USER GUIDE

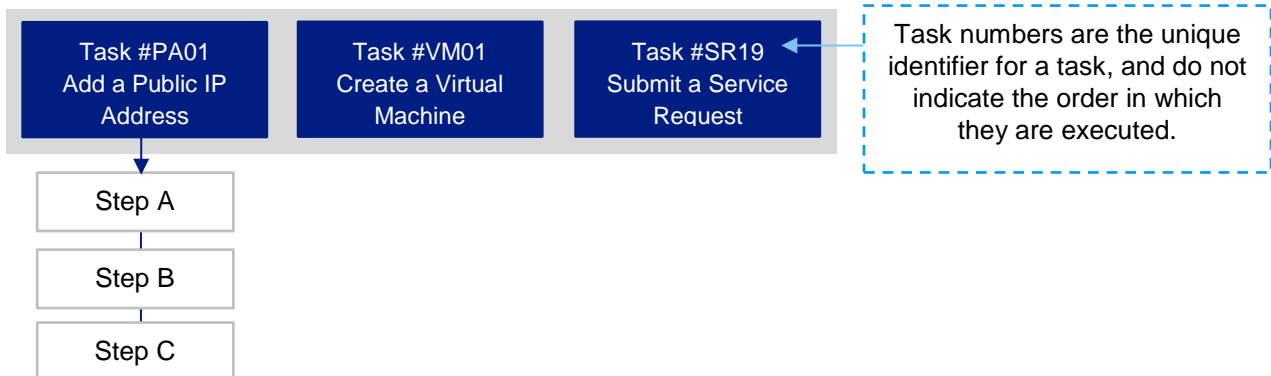
This guide will help you navigate and complete critical tasks and provide tips to better utilise your Telstra Cloud Infrastructure. This guide includes instructions on how to manage and maintain your dedicated Telstra Cloud Infrastructure to create and modify virtual servers and manage your network connections.

This guide is specific to customers uplifted from Virtual Server (Dedicated) Gen1 or Gen2 to [Virtual Server \(Dedicated\) Gen2+](#).

TERMINOLOGY USED IN THIS GUIDE

JOB	Equivalent to a Use Case in Virtual Server (Dedicated) Gen2+. A Job consists of a set of Tasks that collectively achieve a configuration goal for a customer
TASK	One self-contained component of a Job. A given Task might occur within many different Jobs.
PROCEDURE	The set of steps that make up a task.

Example Job: Add a publicly-reachable web server to a tenancy using a new VM on an existing host



Telstra Cloud Infrastructure User Guide, Version 1.0 October 2019

© Telstra Corporation Limited (ABN 33 051 775 556) 2012. All rights reserved.

This work is copyright. Apart from any use as permitted under the Copyright Act 1968, information contained within this manual cannot be used for any other purpose other than the purpose for which it was released. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without the written permission of Telstra Corporation Limited.

WHAT'S INSIDE

CHAPTER 1	WHAT IS VIRTUAL SERVER (DEDICATED) GEN2+?	6
	Physical Environment	6
	Logical Environment	6
CHAPTER 2	OUR DATA CENTRES	8
	Telstra's Data Centre Infrastructure	8
CHAPTER 3	YOUR CSX GEN2+ VIRTUAL DATA CENTRES	11
	What is a Virtual Data Centre?	11
	How Do you Connect Privately to your Virtual Data Centre?	12
	Telstra Cloud Gateway	13
	Telstra's Next IP Network	13
CHAPTER 4	TELSTRA UPLIFT TASKS	14
	How Can I Tell Which Product I Use Prior to Uplift?	14
	Uplift from Virtual Server (Dedicated) Gen1	15
	Uplift from Virtual Server (Dedicated) Gen2	15
	Administrative Uplift Outcomes	16
	Administrative Configuration Warnings	16
	Post-Uplift Communication From Telstra to You	16
CHAPTER 5	MANAGING YOUR CSX GEN2+ VDC	17
	Tools to Order, Build and Manage Your vDC	17
	Logging Into vSphere	18
	Logging in for the first time	20
	vDC Alarms	21
CHAPTER 6	VDC EXTERNAL INTERCONNECTS	22
	Public Interconnect	23
	Public Interconnect Addressing	23
	Public Interconnect Routing	24
	Security Considerations for the Public Interconnect	24
	Dedicated Public ESG	25
	Private Interconnect	26
	Dedicated Private ESG	29

CHAPTER 7	VDC TOPOLOGIES	30
	Basic Topologies	30
	Public	30
	Private	32
	Complex Topologies	34
CHAPTER 8	UPLIFT CONSIDERATIONS	36
	NSX Firewall	36
	What is the NSX Firewall?	36
	Post-Uplift View	37
	Security Groups	38
	Private Virtual Machines	39
	Shared Public Network Migration	40
	Load Balancers	41
	DRS Affinity Rules	43
	Pre-Uplift View	44
	Post-Uplift View	44
	Layer-2 Stretch	45
CHAPTER 9	USING AN EMAIL SERVER IN CSX GEN2+	46
	Overview	46
	Request an SMTP Mail Relay from Telstra	46
	Approved External Products	46
CHAPTER 10	JOB EXAMPLES	47
	Overview of Jobs	47
	Job #1: Add a Virtual Server to a Public Network	48
	Job #2: Add a Virtual Server to a Private Network	49
	Job #3: Add a Virtual Server with new storage	50
CHAPTER 11	HOST TASKS	52
	Task #HS01: Add a Host	52
	Task #HS02: Remove a Host	56
CHAPTER 12	STORAGE TASKS	58
	Task #ST01: Add Storage	58
	Task #ST02: Remove Storage	61
CHAPTER 13	PUBLIC ADDRESSING TASKS	63
	Task #PA01: Add a Public IP Address (Range)	63

Task #PA02: Remove a Public IP Address	65
--	----

CHAPTER 14 SERVICE REQUEST TASKS **67**

Task #SR01: Configure Backup	67
Task #SR02: Modify Backup	70
Task #SR03: Add Application to Backup	73
Task #SR04: Add Disk to Backup	76
Task #SR05: Restore from Backup	78
Task #SR06: Manage Backup Accounts	81
Task #SR07: Modify IPsec	83
Task #SR08: Delete IPsec	85
Task #SR09: Request Current Load Balancer Configuration	87
Task #SR10: Modify Load Balancer	89
Task #SR11: Remove Load Balancer	91
Task #SR12: Add SMTP Relay	93
Task #SR13: Remove SMTP Relay	95
Task #SR14: Connect to Next IP	97
Task #SR15: Import Data	99
Task #SR16: Export Data	101
Task #SR17: Update Account Contact Details	103
Task #SR18: Update Technical Contact Details	105
Task #SR19: Submit a Non-Specific Service Request	107

CHAPTER 15 NSX TASKS **109**

Task #NS01: Add a Logical Switch	109
Task #NS02: Add an Edge Services Gateway	111
Task #NS03: Add Distributed Logical Router	114
Task #NS04: Connect a VM to a Logical Switch	116
Task #NS05: Connect aN ESG or DLR to a Logical Switch	117
Task #NS06: Modify NSX Firewall	119
Task #NS07: Add L2 VPN	121
Task #NS08: Add a Load Balancer	122

CHAPTER 16 VCENTER TASKS **124**

Task #VM01: Create a Virtual Machine	124
Task #VM02: Create a VM DRS GROUP	126
Task #VM03: Create a Host DRS GROUP	127
Task #VM04: Create a VM-Host Affinity Rule	128
Task #VM05: Create a VM-VM Affinity Rule	130

Chapter 1

WHAT IS VIRTUAL SERVER (DEDICATED) GEN2+?

Virtual Server (Dedicated) Generation 2 Plus is the newest generation of Telstra's premium public cloud infrastructure products. It runs on our CSX Generation 2 Plus IaaS platform, which we have built using equipment and software from best-in-breed vendors such as Cisco, Juniper Networks, HP, VMware, Dell EMC and NetApp.

Virtual Server (Dedicated) Gen2+ offers you a number of enhancements over previous versions:

- An evolving range of dedicated physical hosts
- Powerful virtualisation capabilities
- Flexible resource topologies
- Broad connectivity to other products and networks
- Smarter provisioning through inbuilt automation
- A consistent management interface and additional support for self-service adds, moves and changes through increased use of native VMware vSphere and NSX functionality.

PHYSICAL ENVIRONMENT

Your Virtual Server (Dedicated) Gen2+ service includes a minimum of two hosts kept physically separate from those of other DC tenants. You can submit orders to add or remove hosts as your processing needs evolve. The processing capacity of each host is dedicated to you, making the management of processing capacity more straightforward and predictable. Telstra manages the physical environment according to defined service level agreements.

Your hosts attach to a high speed network that links them to external private and public networks such as Next IP, Cloud Gateway and Telstra Internet Direct. It also provides a high-speed path to our premium storage infrastructure from Dell EMC and NetApp.

All of Telstra's CSX Generation 2 Plus IDCs offer high availability operation and 24 x 7 security.

LOGICAL ENVIRONMENT

Our CSX Generation 2 Plus infrastructure extensively uses data centre virtualisation software from VMware, including ESXi, vCenter and NSX. When you use Virtual Server (Dedicated) Gen2+, you have a greater ability to define, configure and manage your own physical and logical resources than in any previous versions of the product. For example, you can:

- Define your own VMs
- Construct and configure your own logical network connections and addressing assignments
- Define traffic security and load management policies for traffic entering or leaving your tenancy via a public or private interconnection
- Add and remove storage

- Install and manage your own operating systems, middleware and applications.

In a significant enhancement, Virtual Server (Dedicated) Gen2+ allows you to use VMware’s native systems to configure and manage your tenancy. You will execute most tenancy management functions using vSphere, including some features available through a Telstra-installed vSphere Plug-in.

While you have more direct management and configuration control over your tenancy than ever before, Telstra still reserves certain key functions for our Operations staff to ensure the ongoing security and reliability of CSX Generation 2 Plus for all customers.

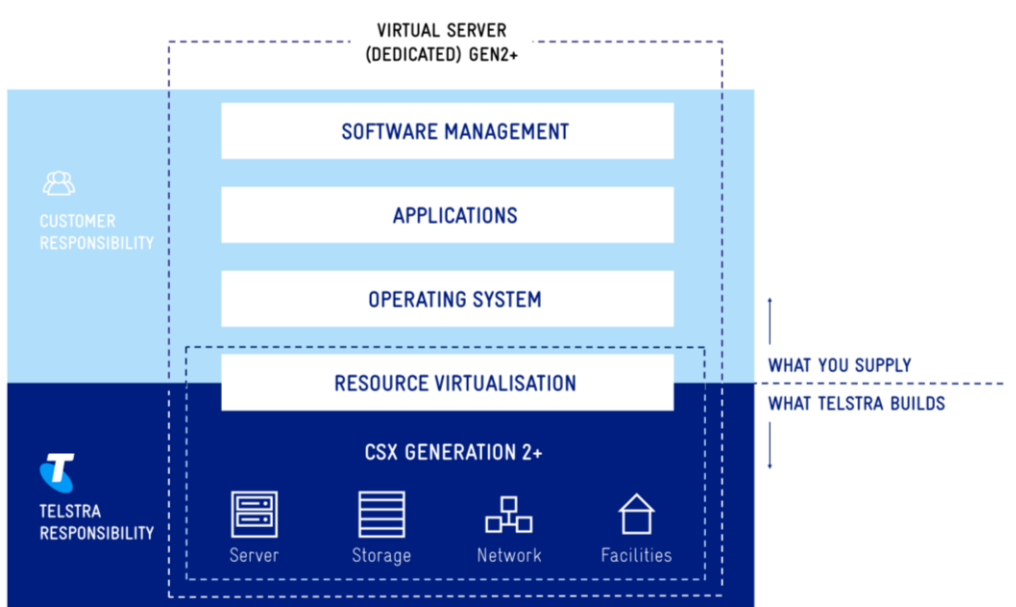


Figure 1: Virtual Server (Dedicated) Gen2+ Component Stack

CUSTOMER ISOLATION

Your data and virtual resources are separated from other customers on three layers – network, compute and data.

ISOLATION LAYER	HOW THIS IS ACHIEVED
NETWORK ISOLATION	Within our DCs we maintain low-level network separation between customers using carrier-grade equipment and technologies. We employ encrypted external communication channels (SSL and IPsec VPN) for management access from public networks. Our transit networks between customers’ virtual servers and data storage areas are isolated from customer networks.
COMPUTE ISOLATION	You are the sole occupant and user of every host you purchase. This maintains physical computing separation between customers in our DCs.
DATA ISOLATION	We dedicate entire volumes to a single customer.

Table 1: Customer Isolation Levels

Chapter 2

OUR DATA CENTRES

TELSTRA'S DATA CENTRE INFRASTRUCTURE

Telstra owns, operates and maintains all the Internet Data Centres (IDCs) that contain the CSX Gen 2 Plus resources and infrastructure supporting cloud products including Virtual Server (Dedicated) Gen2+.

LOCATIONS

Telstra operates CSX Gen 2 Plus IDCs in:

- Melbourne (Clayton)
- Perth (Gnangara)
- Sydney (St. Leonards).

You select which data centre(s) will house your cloud infrastructure services when you buy Virtual Server (Dedicated) Gen2+.



Figure 2: Telstra's CSX Gen 2 Plus Data Centre Locations

PHYSICAL SECURITY

Telstra uses four layers of general security to protect physical infrastructure within our IDCs:

- The outer perimeter of the facility is securely fenced, with the grounds of the site only accessible through a manned gate
- Site grounds are covered by CCTV surveillance
- The IDC building is only accessible through a manned desk with a formal sign-in/sign-out process. Each floor is electronically secured with CCTV surveillance of corridors
- Where an IDC is accessible to customers (such as for Co-Lo facilities) internal rooms contain CCTV surveillance and each cabinet is locked. Customers are escorted to their specific cabinet(s) by a guard who then unlocks them.

Rooms containing CSX Gen 2 plus equipment do not house customer-accessible facilities. The only personnel entering the rooms are authorised Telstra staff or contractors, or support staff from one of our technology partners.

While Telstra does not publicly assert that the IDCs comply with any international standards for data centres, CSX Gen 2 plus-based services have been officially audited for information security management and found to meet ISO 27001.

CONNECTIVITY

Our CSX Gen 2 Plus IDCs provide you with connectivity to:

- The Internet via Telstra Internet Direct
- Internet-attached hosts and sites using an SSL or IPsec VPN tunnel
- Your private networks, supported third-party public clouds and value-added products like Telstra Managed Backup and Telstra Virtual Storage, via Cloud Gateway (Melbourne and Sydney only) or Telstra Next IP VPN (Perth)
- Your data in CSX storage grids
- Your dedicated infrastructure resources.

BACKUP SERVICES

We offer a carrier-grade data backup solution called Telstra Managed Backup (TMB). Built and maintained in partnership with Dell EMC, it is ideal for use with Virtual Server (Dedicated) Gen1/2/2+ and to backup data at other sites within your private network.

Telstra operates backup silos in a number of domestic and international locations. When you use TMB with Virtual Server (Dedicated) Gen1/Gen2/Gen2+, we configure your service to store your backups at a location that is physically separated from the DC housing your production data:

VIRTUAL SERVER (DEDICATED) DC LOCATION	TELSTRA MANAGED BACKUP DC LOCATION
CLAYTON (VIC)	EXHIBITION / BOX HILL
ST. LEONARDS (NSW)	PITT / HOMEBUSH
GNANGARA (WA)	WELLINGTON

Table 2: TMB Storage Locations

AVAILABILITY AND RELIABILITY

Our CSX Generation 2 Plus infrastructure is fully redundant to protect your services and data from a single point of failure. It allows us to provide you with highly resilient and available cloud services.

Telstra's Cloud Services support team continuously monitors our IDC infrastructure using advanced tools and denial of service (DoS) protection.

We maintain network reliability through redundancy on two levels:

1. *Intra-component redundancy* - including dual supervisor engines, multiple power supplies served by diverse power sources and fan redundancy
2. *Inter-component redundancy* - including dual physical components and multiple links

Service level agreements can be viewed in [Our Customer Terms](#) (Australian customers only) or your separate agreement with us.

NETWORK SECURITY

Our IDCs are monitored around the clock by Telstra's team of security specialists, covering:

- The physical infrastructure that provides your cloud services
- Data isolation and privacy between our customers and/or other tenants
- Basic infrastructure and network-level security controls
- Infrastructure logging, alerting and auditing.

Some of the security features of our cloud services infrastructure include:

- Embedded firewalls
- Remote access security
- Regular vulnerability checks
- Denial of service protection
- Privacy controls.

We maintain our security standards by:

- Using leading technologies to perform regular network and infrastructure security updates and
- Engaging a specialist third-party organisation to perform regular penetration testing of our platform.

In addition to the security measures our infrastructure provides, you can customise and enhance your own cloud network security.

Chapter 3

YOUR CSX GEN2+ VIRTUAL DATA CENTRES

WHAT IS A VIRTUAL DATA CENTRE?

A **virtual data centre** (vDC) is another name for a Virtual Server (Dedicated) Gen2+ **tenancy**. It holds cloud resources you have purchased and/or configured in one of our physical data centres. By default, every vDC is logically isolated from the others and can only communicate with one or more of them if you choose to allow it.

Some resources in each vDC are physical and some are logical. Examples include:

- Hosts you have purchased
- VMs you have configured
- Public IP address ranges you have requested from Telstra and used in your vDC topology
- Private IP address ranges you have selected and configured in your vDC topology
- ESGs defined by Telstra or you to perform routing, firewalling and/or load balancing
- Connections to the Internet and/or to Cloud Gateway/Next IP.

Many customers only need and use one vDC but you can have more if you need. For example, you may want to have one vDC in Melbourne and another in Perth to improve performance and/or provide redundancy. And while less common, you can also acquire multiple vDCs in the same physical DC.

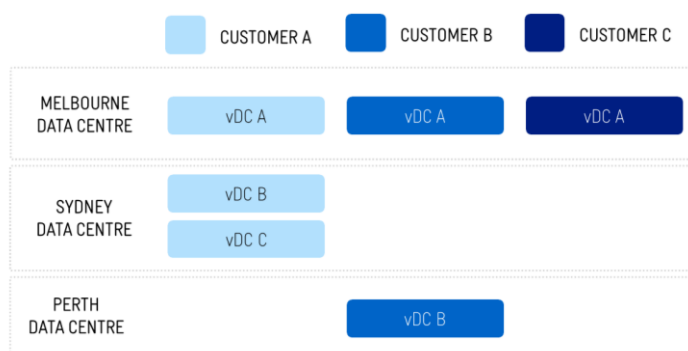


Figure 3: Relationship Between Virtual DCs and Physical DCs

Each physical and logical resource you purchase or configure sits in one vDC. If you have more than one vDC, we determine the vDC containing your resource quite simply: it is the one shown in your vSphere client at the time of purchase or configuration. Consequently, you cannot order or configure a resource in one vDC from a vSphere client logged into another vDC.

For example, you will need have logged into the correct vDC using vSphere when:

- Buying one or more hosts
- Defining VMs on a particular host

- Purchasing a public IP address range to use in a particular vDC
- Configuring logical resources in your vDC.

Importantly, if you purchase and use multiple vDCs, they will initially behave as though they belong to different customers. By default, they will not be able to communicate with each other unless you permit routing between them through external interconnections.

If you want them to be able to communicate, you will encounter architectural restrictions on if, and how, it can occur. Those restrictions are based on where the vDCs reside. The following table summarises the default restrictions on communication between vDCs.¹

PHYSICAL DATA CENTRE 1 CONTAINS...	PHYSICAL DATA CENTRE 2 CONTAINS...	TRAFFIC REACHABILITY BETWEEN VDCS	
		THROUGH CLOUD GATEWAY / NEXT IP	OVER TELSTRA INTERNET DIRECT
vDC X	vDC Y	vDC X <-> vDC Y	vDC X <-> vDC Y
vDC X vDC Y		None	vDC X <-> vDC Y
vDC X vDC Y	vDC Z	vDC X <-> vDC Z vDC Y <-> vDC Z	vDC X <-> vDC Y vDC X <-> vDC Z vDC Y <-> vDC Z

Table 3: Traffic Reachability Between vDCs

If you choose to allow vDCs to communicate with each other or to external networks, it is up to you to design and implement security mechanisms to protect each of them. You might do this with VMware resources such as a distributed firewall and/or by installing and running third party security software in your vDC(s).

HOW DO YOU CONNECT PRIVATELY TO YOUR VIRTUAL DATA CENTRE?

Many of Telstra's Virtual Server (Dedicated) customers want to connect privately from their Next IP VPN to their vDC. Telstra builds each private connection using one of two main methods. The selected method is driven by the combination of vDC location and the generation of Virtual Server (Dedicated) that applied when you first ordered your vDC.

ORIGINAL PRODUCT	LOCATION	EXTERNAL PRIVATE PEERING SERVICE
VIRTUAL SERVER (DEDICATED) GEN1	Sydney or Melbourne	Next IP VPN

¹ There may be advanced configurations that can overcome traffic reachability restrictions shown in the table. However, Telstra does not explicitly support or endorse them

ORIGINAL PRODUCT	LOCATION	EXTERNAL PRIVATE PEERING SERVICE
VIRTUAL SERVER (DEDICATED) GEN2	Sydney or Melbourne	Cloud Gateway
	Perth	Next IP VPN

Table 4: External Private Peering Service for Private Interconnects

Connection via Cloud Gateway has a significant advantage over direct attachment from your Next IP VPN: Cloud Gateway can also seamlessly link several other cloud services from Telstra and our partners using a single interconnection from your Next IP VPN.

TELSTRA CLOUD GATEWAY

Telstra's Cloud Gateway™ is a simple way to access your various cloud platforms including your Virtual Server (Dedicated) vDC. It allows you to log in to a single console, where you can view and manage your cloud connections in one place.

Having all connections in one place makes it easier to understand the relationships between your Telstra private networks and your cloud services.

Whether you're connecting to one or multiple cloud platforms – or adopting a hybrid cloud strategy – Cloud Gateway offers a simple, one-stop solution that you can scale as your workloads change and your business grows.

You must register for the [Cloud Services Store](#) to purchase Cloud Gateway. See the [Cloud Gateway User Guide](#) for details on how to register, connect and disconnect your cloud service to the Cloud Gateway network.

TELSTRA'S NEXT IP NETWORK

A Telstra Next IP private interconnection provides a secure way to connect your VPN-attached sites to your vDC. The private interconnection is a direct, permanent MPLS link between your Next IP VPN and vDC. If you use multiple vDCs, you will need a separate Telstra Next IP private interconnection for each to communicate with it.

You can order a Next IP VPN connection to your vDC using our vSphere Plug-in. Refer to Private Interconnect on page 26 and Task #SR14: Connect to Next IP on page 97 for more information.

Chapter 4

TELSTRA UPLIFT TASKS

When we uplift your existing vDC to Virtual Server (Dedicated) Gen2+ vDC, Telstra will complete certain tasks that upgrade software and make new capabilities available to you. Some of the specific tasks we complete depend on the original product on which you ordered your vDC.

In general terms, we have designed our uplift process to increase the control you have over your vDC and its functionality yet minimise operational disruption and short-term impacts. We do this by upgrading or installing VMware vSphere and NSX software while maintaining your existing resource definitions, addressing and security rules, along with most current topological connections.

HOW CAN I TELL WHICH PRODUCT I USE PRIOR TO UPLIFT?

Virtual Server (Dedicated) Gen2+ is our third iteration of products built on CSX. In general, the names of the CSX infrastructure platforms and our products align:

YEAR LAUNCHED	INFRASTRUCTURE NAME	PRODUCT NAME
2012	CSX (retrospectively known as CSX Generation 1)	Virtual Server (Dedicated) – retrospectively known as Virtual Server (Dedicated) Gen1
2016	CSX Generation 2	Virtual Server (Dedicated) Gen2
2019	CSX Generation 2 Plus	Virtual Server (Dedicated) Gen2+

Table 5: Infrastructure - Product Naming

How can you tell which product you use? There are several potential methods:

- You can check your bill, which does not change after we uplift your vDC:
 - If you use Virtual Server (Dedicated) Gen1, the bill will list “Virtual Server (Dedicated)”. That is, there will not be a generational qualifier
 - If you use Virtual Server (Dedicated) Gen2, the bill will include the generational qualifier (as “Gen2” or “Gen 2”)
- You can check your server infrastructure. CSX Generation 1 uses Cisco M3 hosts, while CSX Generation 2 uses Cisco M4 hosts.

UPLIFT FROM VIRTUAL SERVER (DEDICATED) GEN1

During the uplift of your vDC from Virtual Server (Dedicated) Gen1, Telstra will install some new software packages and upgrade others. The software responsible for certain networking tasks will change. You will have increased authority and permissions to modify many aspects of your vDC network and resources yourself instead of submitting requests to Telstra.

The general tasks comprising this uplift process are:

- a. Install NSX Manager and NSX Controller at the latest validated version
- b. Build your Dedicated Public ESG and Dedicated Private ESG
- c. Replace the Virtual Security Gateway (VSG) with an NSX Distributed Firewall (DFW)
- d. Replace the Nexus 1000v virtual switch with a vSphere Distributed Switch (vDS)
- e. Upgrade vCenter Server to the latest validated version
- f. Register Telstra's vSphere Plug-in
- g. Replace your existing hosts with Cisco M3 hosts running the latest validated version of ESXi. The resource specifications for each new host will match the one it replaces
- h. Migrate your VMs to the new ESXi hosts
- i. Remove old ESXi hosts
- j. Upgrade vSphere Distributed Switch to the latest validated version.

When we migrate the existing VSG to a new NSX DFW, we will carry your security rules across as well.

We do not change certain characteristics of your Virtual Server (Dedicated) Gen1 vDC as a direct result of our uplift activity. For example, we do not alter your load balancers or VPN access. However, you can supplement or replace them later yourself because you will have increased control over your vDC. We discuss this further in upcoming sections.

UPLIFT FROM VIRTUAL SERVER (DEDICATED) GEN2

When we uplift your vDC from Virtual Server (Dedicated) Gen2, the list of tasks we perform is different to that for Virtual Server (Dedicated) Gen1. This is because Virtual Server (Dedicated) Gen2 already uses many VMware packages and features important to Virtual Server (Dedicated) Gen2+, such as NSX and ESGs. But a key outcome is the same: you will have increased authorisations and permissions to modify many aspects of your vDC network and resources yourself, rather than requesting Telstra to complete them.

The general tasks comprising this uplift process are:

- a. Upgrade NSX Manager, NSX Controller and ESGs to the latest validated version
- b. If necessary, build the Dedicated Public ESG (if you currently use a Routed IP Subnet or Floating IP Subnet in your vDC, we will already have built your Dedicated Public ESG)
- c. Upgrade vCenter Server to the latest validated version
- d. Register Telstra's vSphere Plug-in
- e. Replace your existing hosts with Cisco M4 hosts running the latest validated version of ESXi. The resource specifications for each new host will match the one it replaces
- f. Migrate your VMs to the new ESXi hosts
- g. Remove old ESXi hosts
- h. Upgrade vSphere Distributed Switch to the latest validated version.

We do not change certain characteristics of your Virtual Server (Dedicated) Gen2 vDC as a direct result of our uplift activity. For example, we do not alter your VPN access. However, you can supplement or replace them later yourself because you will have increased control over your vDC. We discuss this further in upcoming sections.

ADMINISTRATIVE UPLIFT OUTCOMES

After we uplift your vDC from either Virtual Server (Dedicated) Gen1 or Gen2, you will use different or updated tools and have multiple standard usernames and authorisations to manage it. We cover this in more detail in the next chapter of this guide, but in summary:

- When you first purchased Virtual Server (Dedicated) Gen1 or Gen2, we provided you with a set of administrative usernames to manage your vDC using vSphere. The usernames remain but their permissions change
- Telstra will provide you with the URL for your vSphere client portal plus a new standard administrative username specifically for managing NSX
- You will be able to use the vSphere HTML5 web client and/or Flex client
- Our vSphere Plug-in will appear in your vSphere HTML5 web client (but not the Flex client). You can use this plug-in to order new hosts, storage or public IP addresses for your vDC, or to remove them. You can also submit other assorted service requests.

ADMINISTRATIVE CONFIGURATION WARNINGS

When you assume administrative control of your vDC after uplift, you will see a significant increase in your permissions and authority to make changes. We set your permissions using role-based access control (RBAC) parameters in vCenter and NSX.

Some RBAC settings that are necessary to give you access to important vCenter and NSX functions also permit actions that you do not actually need to use with Virtual Server (Dedicated) Gen2+, and can even impair the operation of your vDC if you misconfigure them. For example, your administrative permissions allow you to manipulate the NSX 'Installation and Upgrade' menus and panels. However, there are no settings or parameters that you should need to touch in this area.

If you do make changes to settings that disrupt your vDC, Telstra reserves the right to charge a service fee to reinstate the correct configuration.

POST-UPLIFT COMMUNICATION FROM TELSTRA TO YOU

After we complete the uplift process for your vDC, we will email a *welcome letter* to you. This letter provides important information about your Virtual Server (Dedicated) Gen2+ vDC and its resources, such as:

- The Service ID (also called a Subscription ID or Tenancy ID) for your vDC
- Your Account Name
- The Usernames for your additional vSphere administration account
- The URL for your vSphere client portal. This portal supports both the HTML5 client (recommended) and the Flex web client
- Support and contact information for Telstra Operations.

You will receive a separate email containing the initial passwords for your additional vSphere administration account.

Chapter 5

MANAGING YOUR CSX GEN2+ VDC

Virtual Server (Dedicated) Gen2+ employs a 'shared responsibility' philosophy to allow you to configure and control most of the resources in your vDC. We use role-based access control (RBAC) in vSphere for both vCenter and NSX to restrict access to features and functions that are not available to you.

TOOLS TO ORDER, BUILD AND MANAGE YOUR VDC

You will use a vSphere client to co-manage your vDC through vCenter. We can support either

- a. vSphere client (HTML5) – this is our recommended choice
- b. vSphere Web Client (VMware also calls this the **Flex client**) – we do not recommend this client but you may occasionally need to use it to execute a small number of administration tasks not supported by the HTML5 client. It does not offer the Telstra vSphere Plug-in.

Using either of these clients allows you to control the provisioning, configuration, operation and release of VMs, ESGs and certain other VMware virtual devices without Telstra's intervention.

VMWARE SOFTWARE VERSIONS

Virtual Server (Dedicated) Gen2+ uses the following versions of VMware software:

- vSphere version 6.7, comprising:
 - vCenter Server
 - ESXi Server
 - vSphere client (HTML5) or web client (Flex)
- NSX version 6.4.

In order to manage your vDC using vCenter Server or NSX, you must login with the correct username for the tasks you plan to complete. The vSphere client will generally show all high-level menu options for both vCenter Server and NSX for every username, but you cannot see or choose options for vCenter Server if you have logged in with the NSX username, and vice-versa. For example, when you need to manage your host resources, such as to provision or reconfigure a VM, you will use the vSphere client to login with a username for vCenter Server. If you need to manage your network configurations, such as those for Logical Switches, ESGs or DLRs, you will use the vSphere client to login with a username for NSX Manager.

TELSTRA-SUPPLIED TOOLS

In the past, Telstra provided the Cloud Services Management Console (CSMC) to allow you to request configuration services for Virtual Server (Dedicated) Gen1 and Gen2. Many of the actions available on the CSMC become directly configurable by you once we uplift your vDC. However, there are still some requests that we must complete for you.

Telstra has built a vSphere Plug-in utility to replace your Cloud Services Management Console (CSMC). We register this with your vSphere management environment when we uplift your vDC. The plug-in appears as a selectable icon in the vSphere client. Once uplifted, you will use Telstra's vSphere Plug-in to submit requests for these actions:

Host Requests

Storage
Requests

Public IP
Address
Requests

Service
Requests

We cover how to submit these requests later in this guide.

USERNAMES

You will use a set of pre-defined usernames to manage your vDC. We provided some of these usernames to you when we commissioned your original Virtual Server (Dedicated) Gen1 or Gen2 vDC. We provide the rest when we uplift your vDC.

Telstra relies on inbuilt VMware role-based access control (RBAC) to permit or disable specific management tasks. Each username has specific permissions for either vCenter Server or NSX. If you plan to complete host-related tasks, you will login to vSphere with a username offering read-write management of vCenter Server. Conversely, if you plan to complete network-related tasks, you will login to vSphere with a read-write username for NSX. There is also a read-only username for basic monitoring and reporting access to vCenter Server.

The following table outlines the usernames and their capabilities.

LOGIN NAME(S)	PERMISSIONS
admin@c[clientnumber].csx admin2@c[clientnumber].csx admin3@c[clientnumber].csx admin4@c[clientnumber].csx admin5@c[clientnumber].csx	Read-write access to Hosts and Clusters (vCenter)
networkadmin@c[clientnumber].csx	Read-write access to Networking and Security (NSX)
readonly@c[clientnumber].csx	Read-only access for monitoring and reporting on Hosts and Clusters (vCenter)

Table 6: Username Permissions for vSphere

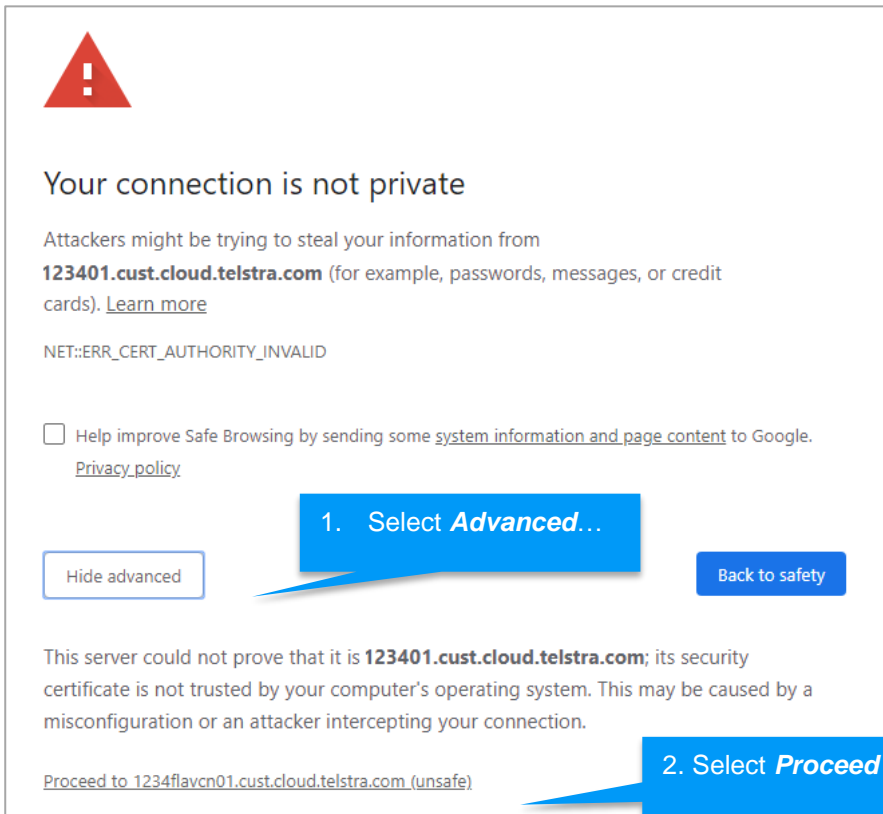
LOGGING INTO VSPHERE

When you login to vSphere, you will contact a URL that is specific to your vDC. We will provide the URL to you after we uplift your vDC to Virtual Server (Dedicated) Gen2+.

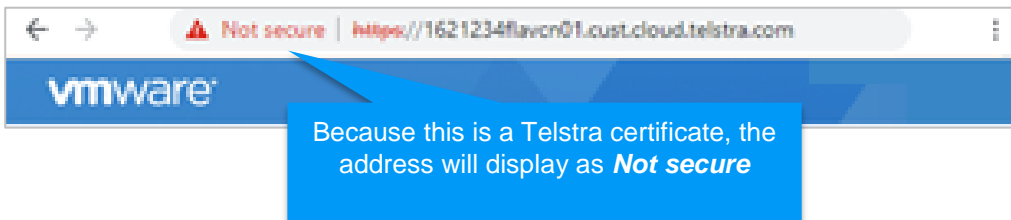
We recommend that you use the latest version of the Chrome browser with the vSphere client. We have not tested or validated other browsers with Virtual Server (Dedicated) Gen2+.

Telstra provides a self-signed certificate for HTTPS connections to vSphere. Your browser will complain that this certificate is not issued by a trusted certificate authority and recommend that you do not complete the connection. You will need to proceed with the connection to reach the login panel for vSphere.

For Chrome, you will need to click on 'Advanced' to reveal the 'Proceed' option.



When you reach the panel to select your preferred client, the browser will inform you via the URL line that the site is 'Not secure'. This is only because it does not trust the self-signed certificate.

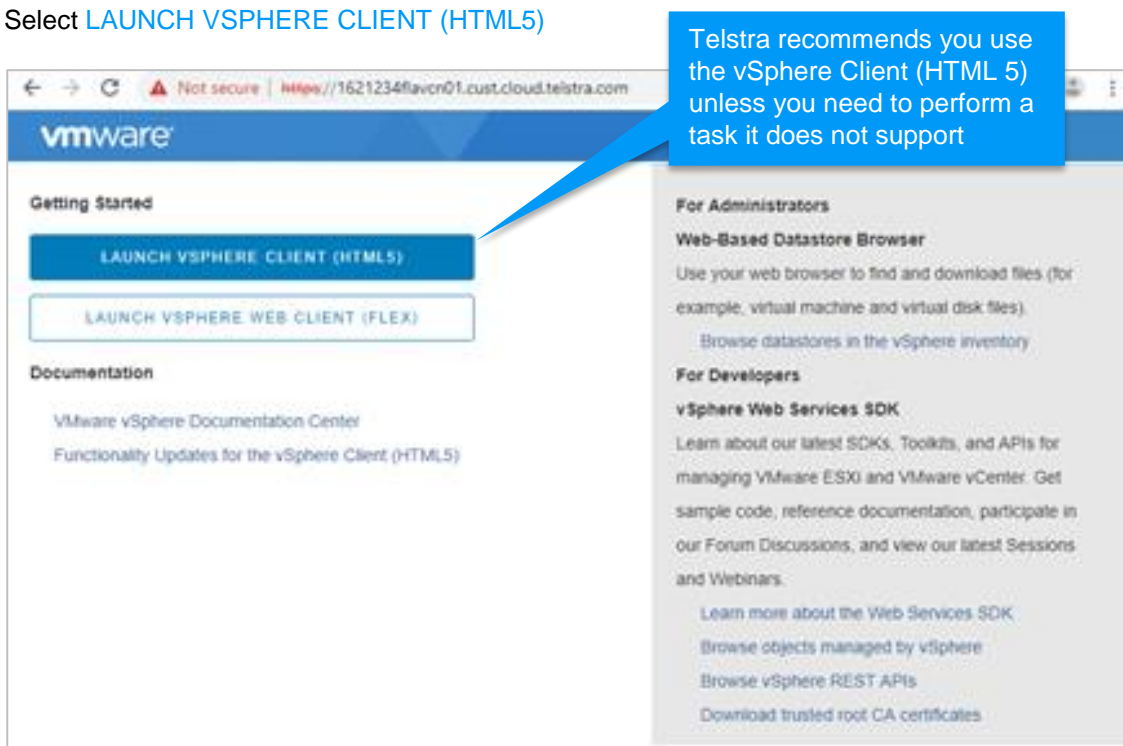


The vSphere Client (HTML5) is a superior way to access vSphere. However, there is a small amount of functionality yet to move across from the Flex Web Client. For Virtual Server (Dedicated) Gen2+, this primarily relates to Edge functions in NSX. Should you need to access this functionality you will need to temporarily access vSphere via Flex.

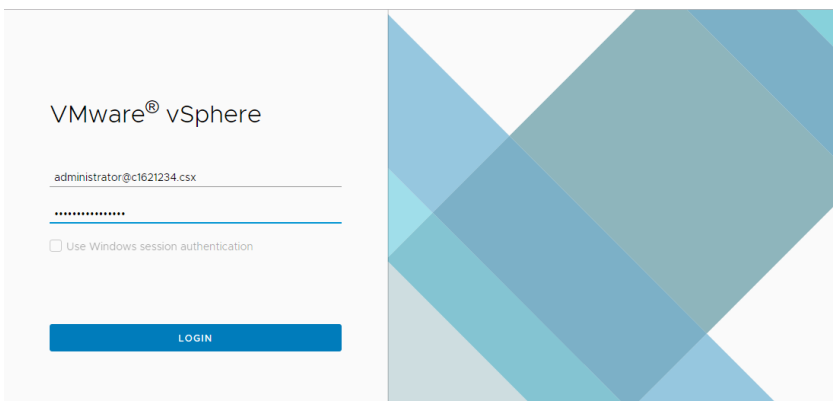
LOGGING IN FOR THE FIRST TIME

STEP 1: LOGIN TO VCENTER

Select [LAUNCH VSPHERE CLIENT \(HTML5\)](#)

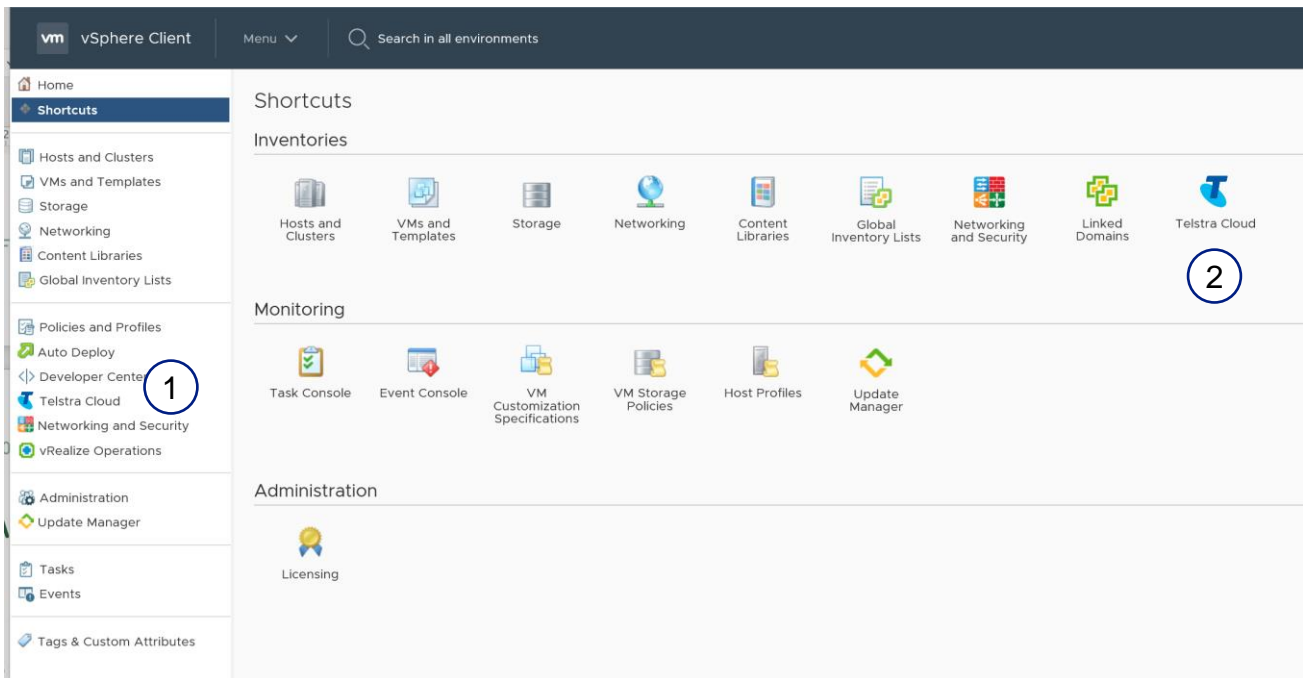


When you login to vSphere, you need to choose a username that matches the tasks you plan to perform. You will enable adds, moves and changes in vCenter Server tasks by logging in using *admin*, *admin2*, *admin3*, *admin4* or *admin5*. To perform adds, moves and changes in NSX, login with *networkadmin*.



You might mostly be using the native vSphere client menu items. If you wish to use Telstra's vSphere Plug-in to submit a request to us, you need to click on its icon. You will find the **Telstra Cloud** icon:

1. In the vSphere client sidebar, and/or
2. On the vSphere client Shortcuts panel.



VDC ALARMS

All hardware and software alarms for your vDC will appear in your vSphere client console. As a result, you can monitor the status of your vDC.

Telstra also monitors some of the alarms from your vDC, but only those related to infrastructure and resources that we directly control. These include:

- Host alarms from ESXi
- Networking alarms
- Other facility alarms
- Storage alarms including those raised as you near to filling your datastore(s)

We do not see or react to alarms related to logical resource management. You will need to ensure that you do not overcommit your host processing capacity or hinder vMotion (DRS and HA) with too many VMs in a cluster, and that you reclaim storage or purchase more as it fills.

Chapter 6

VDC EXTERNAL INTERCONNECTS

Telstra has designed Virtual Server (Dedicated) Gen2+ with a multi-tenancy architecture that offers flexibility with security, privacy and reliability.

Using your vSphere client, you have the ability to configure your vDC's internal topology as you see fit. We do not explicitly restrict the number of VMs and ESGs in your vDC, but you will need to observe VMware's specifications, Telstra's product capabilities and rules, and the practical limits of your physical and logical resources. You can connect your resources together in your preferred network topology and then define and implement the firewall rules to protect them.

Your vDC will typically communicate with outside locations that might include the Internet, a Next IP VPN, other products like Telstra Virtual Storage and Telstra Cloud Backup, and/or third-party public cloud providers. We therefore recommend you become familiar with our design and terminology for external network connections.

If you communicate from your vDC to any destination via the Internet, you will use a Public Interconnect. The Public Interconnect joins a Dedicated Public ESG in your vDC to a HA-pair of Dedicated Public Routers outside of your vDC. Each Dedicated Public Router connects to the Internet via Telstra Internet Direct (TID). Depending on the features you use in your vDC, we may have slightly modified your Public Interconnect when we uplifted it to Virtual Server (Dedicated) Gen2+.

If you communicate from your vDC to a Next IP VPN or any destination reached through Cloud Gateway, you will use a Private Interconnect. The Private Interconnect joins a Dedicated Private ESG in your vDC to a HA-pair of Dedicated Private Routers outside of your vDC. Depending on the features you use in your vDC, we may have slightly modified your Private Interconnect when we uplifted it to Virtual Server (Dedicated) Gen2+.

The upstream external connection from each Dedicated Private Router is determined by the combination of the original purchased product and location of your vDC. Refer to Table 7.

ORIGINAL PRODUCT	LOCATION	EXTERNAL PEER SERVICE
VIRTUAL SERVER (DEDICATED) GEN1	SYDNEY OR MELBOURNE	NEXT IP VPN
VIRTUAL SERVER (DEDICATED) GEN2	SYDNEY OR MELBOURNE	CLOUD GATEWAY
	PERTH	NEXT IP VPN

Table 7: External Peer Service for Private Interconnects

The Dedicated Public ESG and Dedicated Private ESG are logical VM-based devices sitting in your vDC. We configure them with HA features including active/standby VMs to provide your vDC with resilient connectivity across the Public and Private interconnects.

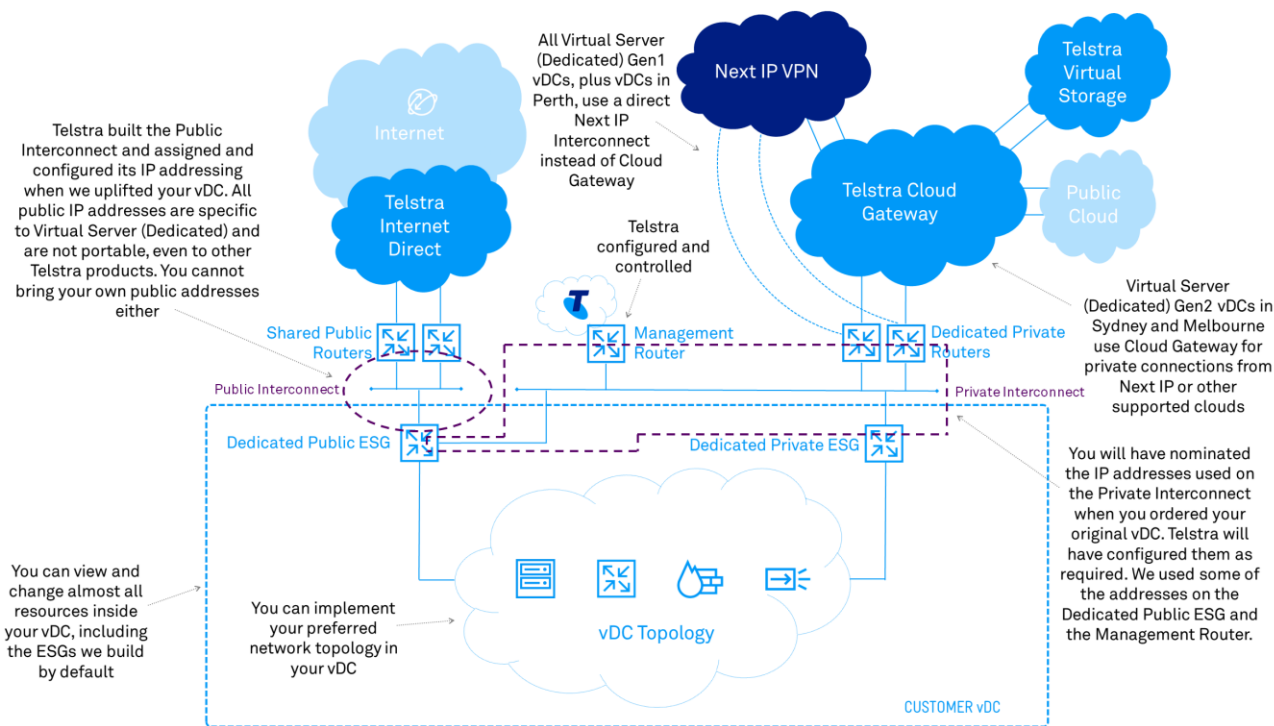


Figure 4: External Network Connections to CSX Gen2+

PUBLIC INTERCONNECT

When Telstra uplifted your Virtual Server (Dedicated) Gen2+ vDC, we included a Public Interconnect that runs from a Dedicated Public ESG in your vDC to Shared Public Routers connected to TID. We assigned and configured the IP addresses for the devices and links that comprise the Public Interconnect. You cannot view or change the configuration of TID or the Shared Public Routers.

The Dedicated Public ESG resides on a host in your vDC. After we complete the uplift, you can see this ESG and inspect or change its configuration, but you need to be careful because you can disrupt its connectivity to the Shared Public Routers if you make a mistake or try to configure a feature or setting we do not support.

PUBLIC INTERCONNECT ADDRESSING

Telstra builds the Public Interconnect using an IP address range that is reserved by IANA specifically for carrier use. It is based on RFC 6598 and drawn from 100.64.0.0/10. You will see this range in use in your Dedicated Public ESG following uplift.

While not identical to the RFC 1918 private addressing ranges you are probably familiar with, the carrier-specific range has similar characteristics because it can be used by any carrier and is not globally routable nor advertisable on public links. We chose to use this range for the Public Interconnect because we expect it to be compatible with your existing network.

Telstra also configures one 'usable' public IP address on your Dedicated Public ESG. We put it on the interface facing the Public Interconnect (ie. to the Shared Public Routers) as a secondary address.

You can use the single public IP address on the Dedicated Public ESG for your own purposes, including for SSL or IPsec VPN tunnel terminations or to apply NAT to traffic entering or leaving your vDC. If you need more than one usable public IP address, you will need to order a range from Telstra (see Task #PA01: Add a Public IP Address (Range) on page 63).

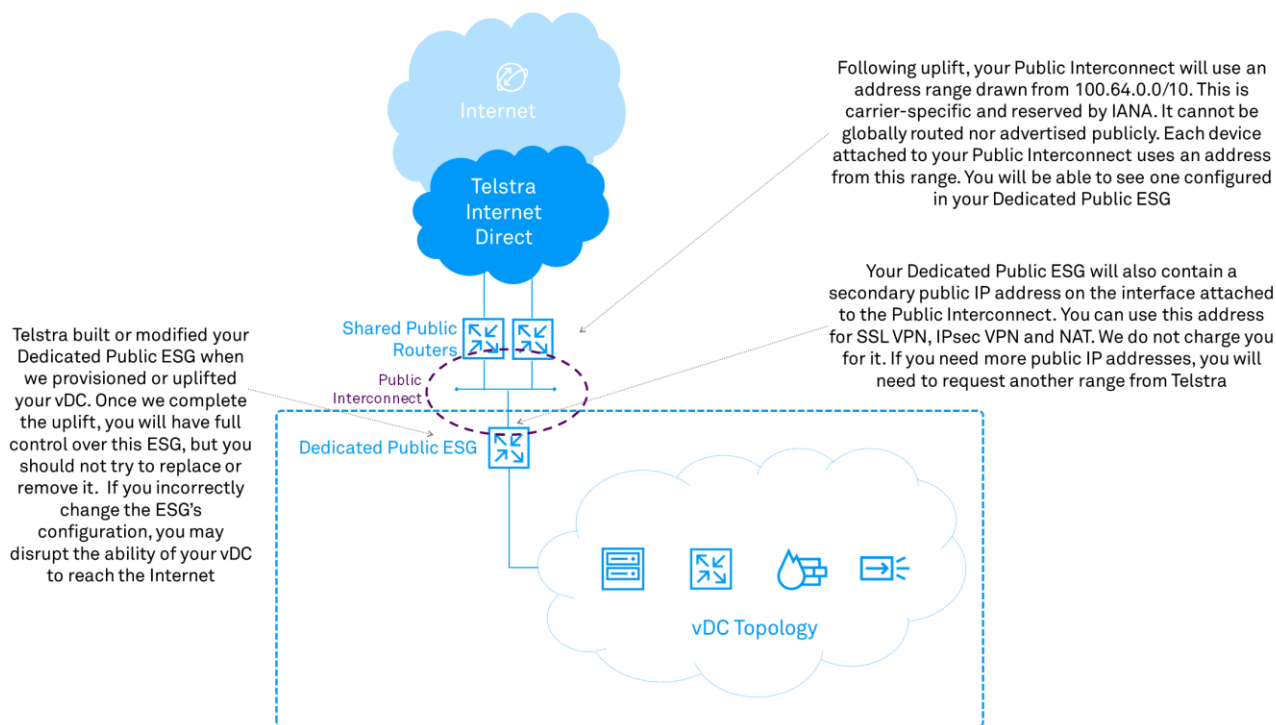


Figure 5: Public Interconnect Addressing

PUBLIC INTERCONNECT ROUTING

The Dedicated Public ESG and Shared Public Routers use static routing. We configure your Dedicated Public ESG with a default route pointing at the HA Virtual IP address (VIP) for the Shared Public Routers when we uplifted your Public Interconnect.

The Shared Public Routers contain a route leading to the single usable public IP address we provide as a secondary interface address in your Dedicated Public ESG when we build your Public Interconnect. If you already had a public IP address range assigned to your vDC when we uplifted it, we will have automatically configured the Shared Public Routers with a static route to that range too. If you subsequently order another range, we will then configure another static route to that range when we provision it. All additional static routes in the Shared Public Routers point to your Dedicated Public ESG. You can then configure your Dedicated Public ESG and/or vDC topology to forward and/or use those ranges.

SECURITY CONSIDERATIONS FOR THE PUBLIC INTERCONNECT

It is up to you to implement firewall rules in your vDC to protect it from external threats. This includes your Dedicated Public ESG and all resources reachable in your vDC behind it. Telstra treats the Public Interconnect as a normal, open Internet access service and we do not configure any default firewalls on it.

You can use the NSX Firewall or a VM containing your preferred virtual firewall appliance to configure and apply security in your vDC. If you had firewall rules configured in a Cisco VSG or NSX Firewall prior to uplift, Telstra will have retained them when we uplifted your vDC. (We will have migrated any Cisco VSG rules to an NSX Firewall during uplift. You can read more about this in the section on NSX Firewall on page 36.) We also recommend you consider the impacts on your firewall rules whenever you modify your vDC topology or resources and then make appropriate adjustments to the DFW.

Under a product rule, outgoing SMTP mail from your vDC must pass through an approved mail relay service. We discuss this in another section of this guide. We also offer various security products that can interwork with CSX Gen2+. Talk to your account team or Telstra partner for more information.

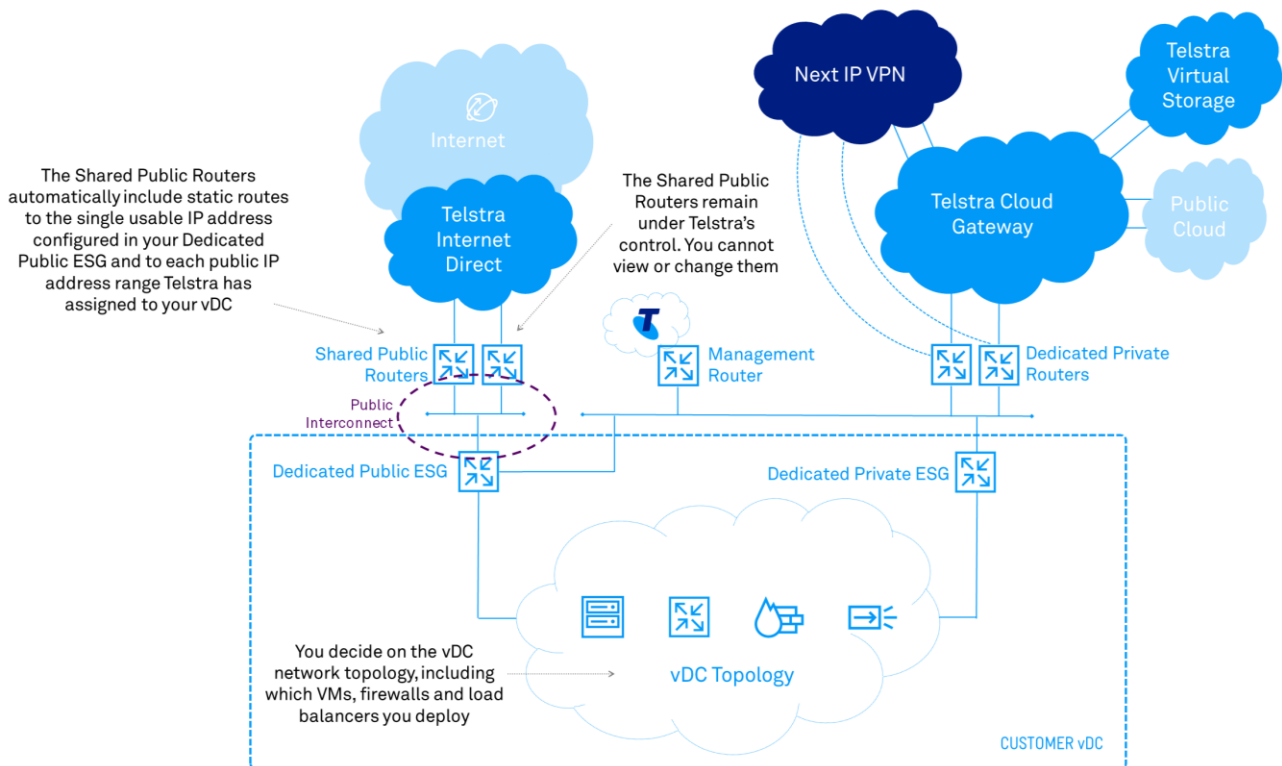


Figure 6: Public Interconnect Routing

DEDICATED PUBLIC ESG

When you login to vSphere with the *networkadmin* username, you can see and modify resources in NSX, including the Dedicated Public ESG. We do not encourage you to change its configuration except where necessary to support your downstream topology.

When using the vSphere client to administer NSX, you can recognise the Dedicated Public ESG by its name which is based on the following template:

```
<service ID>-<location>-<seq_a>-pbded-<seq_b>-VR
```

An example of the name of a Dedicated Public ESG is:

```
9620081-gnan-01-pbded-01-VR
```

The key field to notice is *pbded*, which stands for **Public Dedicated**.

To provide your vDC with resilient operation, we always configure the Dedicated Public ESG in a HA active/standby configuration.

PRIVATE INTERCONNECT

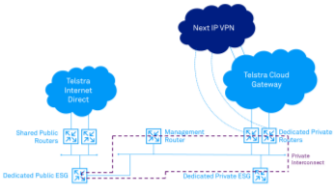
The Private Interconnect runs between the Dedicated Private Routers, Dedicated Private ESG, Management Router and Dedicated Public ESG. The Private Interconnect is integral to several different connections:

- If we uplift you from Virtual Server (Dedicated) Gen2 and your vDC is in Sydney or Melbourne, between your vDC and Cloud Gateway via the Dedicated Private Routers
- If we uplift you from Virtual Server (Dedicated) Gen1 or your vDC is in Perth, between your vDC and Next IP via the Dedicated Private Routers
- Management access via the Management Router:
 - For Telstra Operations to assure your vDC
 - For you to operate your vSphere client
- External SSL VPN and/or IPsec VPN access for your management and/or data traffic crossing the Public Interconnect and through the Dedicated Public ESG.

You will have provided multiple private IP address ranges when you ordered your original vDC and/or your Cloud Gateway or Next IP interconnection. We will have assigned and configured addresses from those ranges to the various connections associated with our vDC. The original product and location of your vDC affects how we will have completed provisioning.

SUPPLY AND USE OF IP ADDRESS RANGES

This table summarises the supply and use of IP address ranges on the Private Interconnect and surrounding links.

ORIGINAL PRODUCT AND VDC LOCATION	CONNECTION SEGMENT	SPECIFIED ON WHICH PRODUCT ORDER?	IP RANGE SIZE
<p>VIRTUAL SERVER (DEDICATED) GEN1 IN SYDNEY OR MELBOURNE</p>	<p>Private Interconnect: the link between Dedicated Private Routers, Dedicated Private ESG, Management Router and Dedicated Public ESG</p> 	<p>N/A</p>	<p>Telstra-supplied range that was compatible with your <u>entire</u> private routing domain</p> <p>Telstra used a standard template to assign addresses from the range to each participating interface</p>

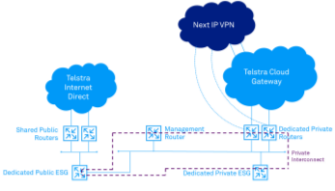


ORIGINAL PRODUCT AND VDC LOCATION	CONNECTION SEGMENT	SPECIFIED ON WHICH PRODUCT ORDER?	IP RANGE SIZE
VIRTUAL SERVER (DEDICATED) GEN2 IN SYDNEY OR MELBOURNE	Private Interconnect: the link between Dedicated Private Routers, Dedicated Private ESG, Management Router and Dedicated Public ESG 	Original Virtual Server (Dedicated) Gen2 product application form	/29 or larger that is compatible with your <u>entire</u> private routing domain Telstra used a standard template to assign addresses from the range to each participating interface
VIRTUAL SERVER (DEDICATED) GEN2 IN SYDNEY OR MELBOURNE	Cloud Gateway to Dedicated Private Routers 	Cloud Gateway when you order a connection to Telstra Virtual Server (Dedicated) Gen2	/29 that was compatible with your <u>entire</u> private routing domain (Telstra segmented into 2 x /30)
VIRTUAL SERVER (DEDICATED) GEN1 OR VIRTUAL SERVER (DEDICATED) GEN2 IN PERTH	Next IP VPN to Dedicated Private Routers 	N/A	Next IP trunk link. No addressing required

Table 8: Addressing on Private Interconnect and Surrounding Links

Telstra will have applied all addresses (from the specified range) to the devices and links that comprise the Private Interconnect. You cannot view or directly change the configuration of Cloud Gateway, the Next IP Interconnect or the Dedicated Private Routers. However, after uplift you will manage all private IP addresses inside your vDC topology. You also specify and new ranges you need in your vDC, and you will need to configure any additional interfaces required in your Dedicated Private ESG.

The Dedicated Private ESG resides on a host in your vDC. You can see this ESG and inspect or change its configuration, but you need to be careful not to make a mistake or try to configure a feature or setting we do not support. This is because you could accidentally disrupt:

- The connectivity from your vDC to the Dedicated Private Routers, or
- Management and/or data access to your vDC using SSL VPN or IPsec VPN via the Dedicated Public ESG.

It is up to you to implement firewall rules in your vDC to protect it from external threats. For your data security, Telstra will have retained your existing firewall rules when we uplifted your vDC. We also recommend you consider the impacts on your firewall rules and make appropriate adjustments or add more security layers whenever you modify your vDC topology or resources. For example, if you employ both

publicly reachable and private resources in your vDC and you link them, you might need to implement advanced security to protect your private networks from threats introduced to your vDC through other means, including through the Public Interconnect.

Telstra offers various security products that can interwork with Virtual Server (Dedicated) Gen2+. Talk to your account team or Telstra partner for more information.

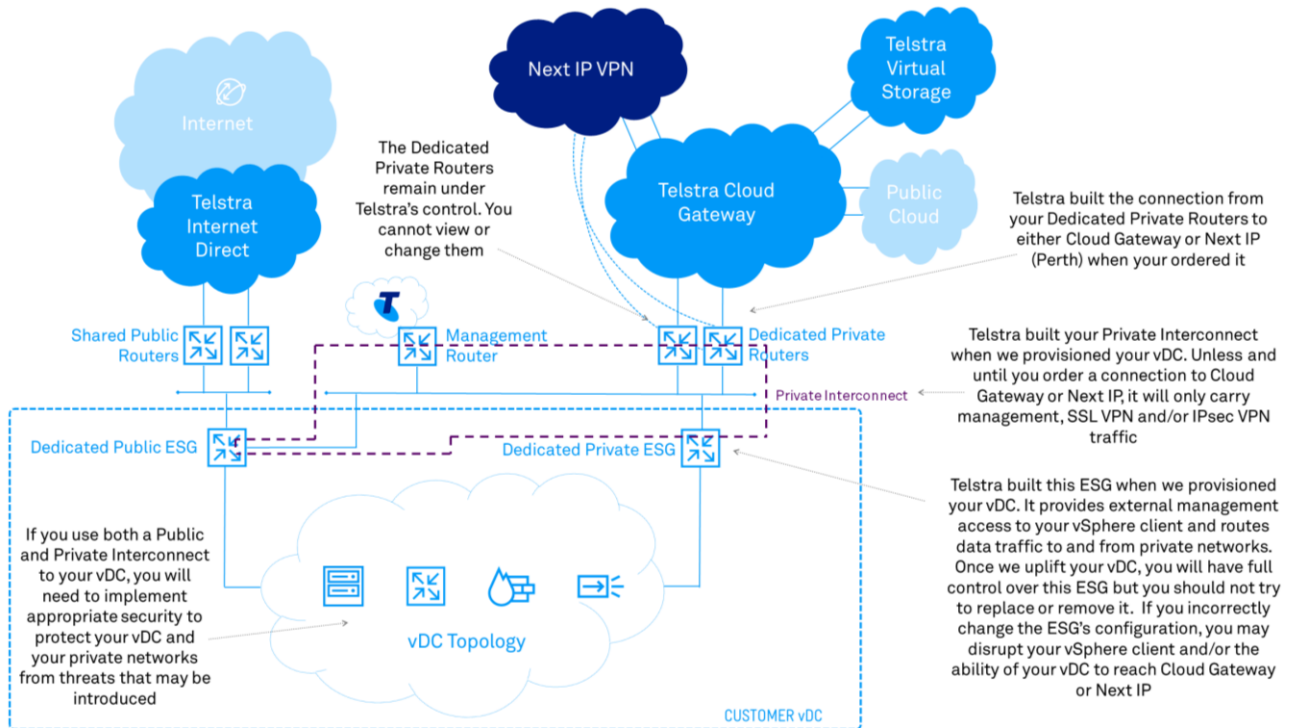


Figure 7: Private Interconnect Overview

The Dedicated Private ESG and Dedicated Private Routers use BGP to exchange routes. You can configure the Dedicated Private ESG to advertise your private IP address ranges to each Dedicated Private Router, which will advertise them to Cloud Gateway or Next IP. The ESG will continue to advertise all routes that were active when we uplifted your vDC.

Outbound advertisements from the Dedicated Private ESG to the Dedicated Private Routers are not filtered. In principle you can advertise any ranges you like, including the default route and public IP ranges, and a Dedicated Private Router will accept and propagate them.

However, you must be mindful of the restrictions on upstream networks. For example, while Cloud Gateway will accept a default route (0.0.0.0/0) it limits the prefix lengths allowed for certain summary and aggregate routes such as 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16 and 0.0.0.0/8. Furthermore, Cloud Gateway will not accept a number of other loopback and link-local ranges. Refer to our product specifications for Cloud Gateway for more information on routing restrictions.

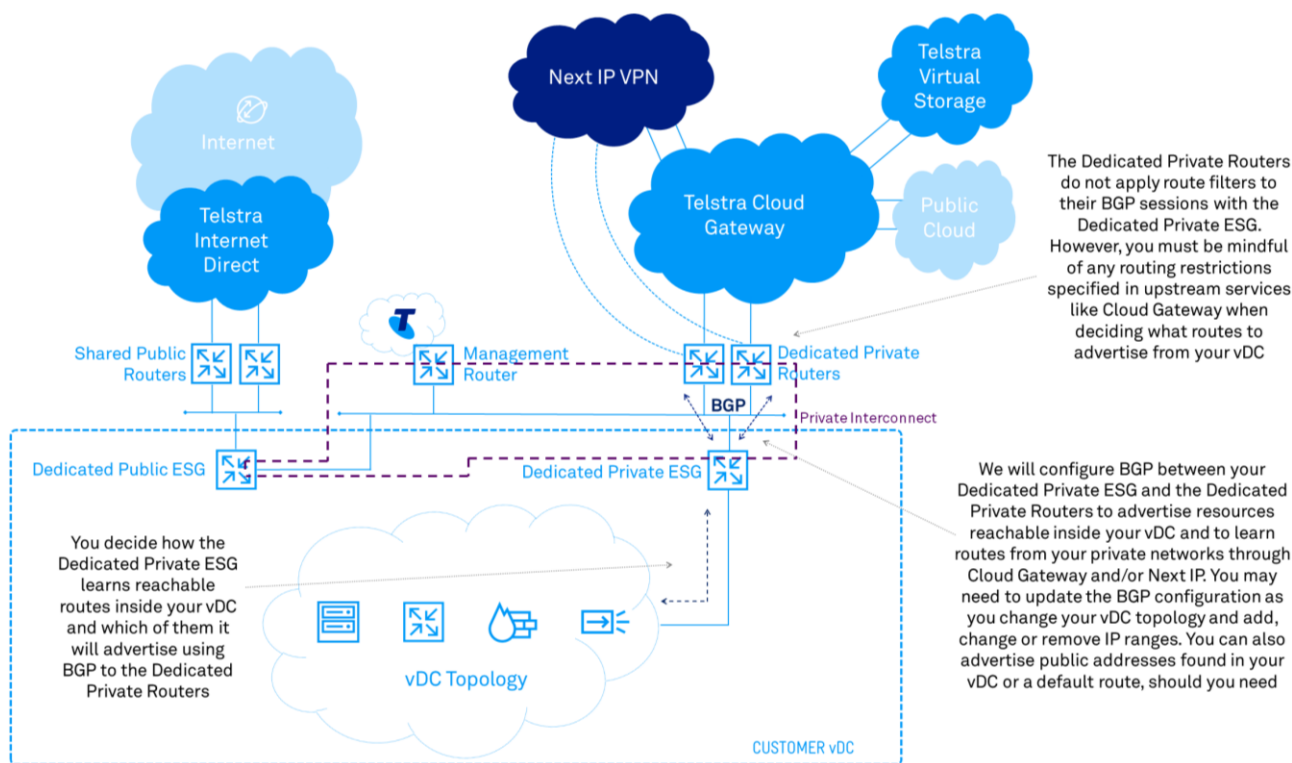


Figure 8: Private Interconnect BGP Routing

DEDICATED PRIVATE ESG

When you login to vSphere with the *networkadmin* username, you can see and modify resources in NSX, including the Dedicated Private ESG. We do not encourage you to change its configuration except where necessary to support your working topology and to advertise routes to the Dedicated Private Routers across the Private Interconnect.

When using the vSphere client to administer NSX, you can recognise the Dedicated Private ESG by its name which is based on the following template:

```
<service ID>-<location>-<seq_a>-sth-<seq_b>-VR
```

An example of the name of a Dedicated Private ESG is:

```
9620081-slen-01-sth-01-VR
```

The key field to notice is *sth*, which indicates that this ESG is connected to the south interfaces on the Dedicated Private Routers.

To provide your vDC with resilient operation, we always configure the Dedicated Private ESG in a HA active/standby configuration.

Chapter 7

VDC TOPOLOGIES

Virtual Server (Dedicated) Gen2+ allows you to define, arrange and connect the logical resources inside your vDC to suit your needs. Beginning with Virtual Server (Dedicated) Gen2+, Telstra will not impose specific design criteria on your vDC except for these special circumstances:

- a. Restrictions necessary to protect the general integrity of our customers' tenancies and our infrastructure
- b. Routing rules that control how your vDC connects to external networks through the Public and Private Interconnects
- c. When we uplifted your vDC from Virtual Server (Dedicated) Gen1, we will have retained legacy Cisco ACE-based load balancers in your service topology if you used them in the past
- d. When we uplifted your vDC from Virtual Server (Dedicated) Gen1 or Gen2, we will have retained an IPsec VPN access termination on your Dedicated Private Routers if you used one in the past.

Even in the latter two cases, you can supplement or replace these resources with others you define in NSX.

Therefore, it is up to you to carefully consider the security, performance, resiliency and cost impacts of your topology. For example, if you make a resource reachable from both the Public Interconnect and Private Interconnect, you have created a path to your vDC and downstream private networks from the Internet, so you will need to implement effective security measures to protect them. Or, if you decide to request a larger number of public addresses for your vDC than you really need, you might needlessly incur higher fee

BASIC TOPOLOGIES

PUBLIC

A basic public topology is one that exclusively communicates with external parties over the Public Interconnect.

In order to make your VMs visible to the Internet over the Public Interconnect, you will need an appropriate range of public IP addresses to use with them. In very simple cases, you can use NAT with your single usable address in the Dedicated Public ESG. If you had public address ranges assigned to your vDC when we uplifted it, they will still be active and assigned to the same resources as they were. Otherwise, you can request an additional range. Should you need one or more further ranges in future, we will assign each to your vDC after you submit a request using our vSphere Plug-in.

If you ordered and received one or more public IP address ranges for use in your vDC, you can configure them on your VMs or other logical devices. It is up to you to determine the appropriate public network topology and to configure workable IP addressing.

Telstra will configure the Dedicated Public ESG with a default route pointing to the Shared Public Routers when we uplift your vDC. We will also configure the Shared Public Routers with a route to each public IP address range assigned to your vDC. We show the standard routing configuration for the Public Interconnect in Figure 9.

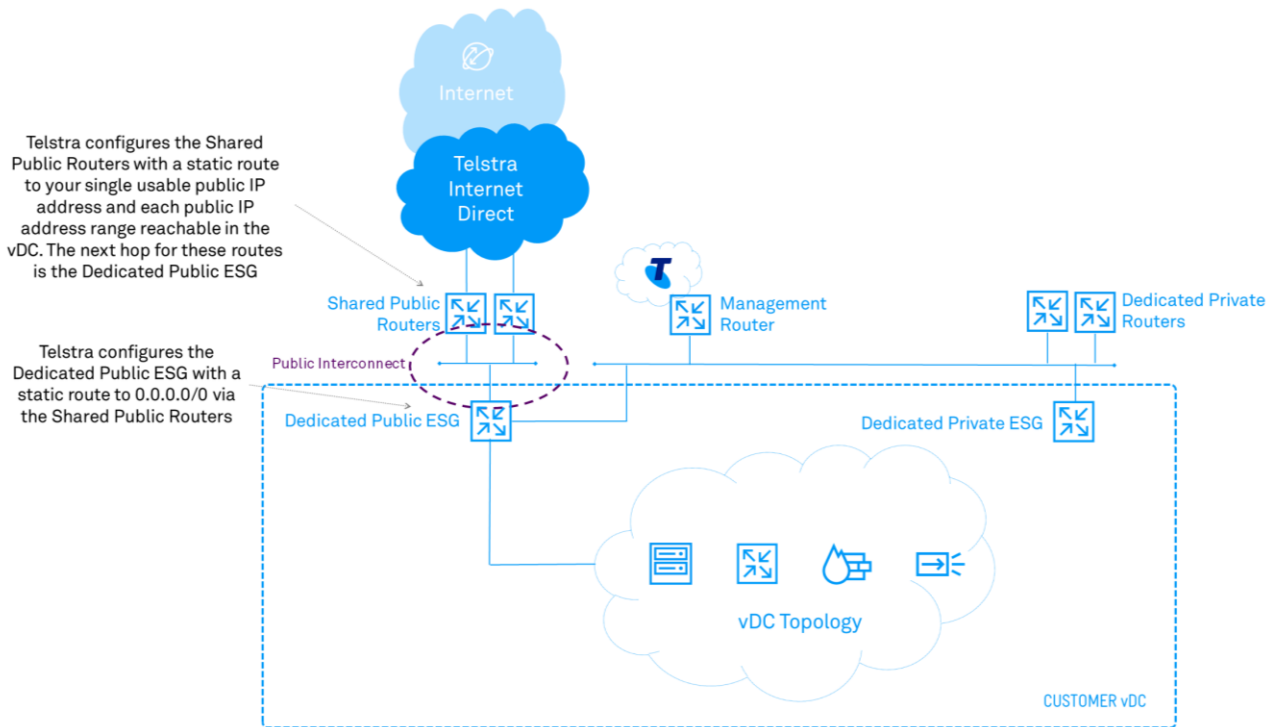


Figure 9: Publicly Reachable Routing Arrangement

In Figure 10, we show a simple basic public topology for example ‘Customer A’. It shows the Dedicated Public ESG and a small number of Internet-facing servers sharing a common LAN segment. The servers each use a public IP address drawn from a small range Customer A has requested through the Telstra Plug-in. After we assigned the public IP range to the vDC in response to Customer A’s request, we configured the static route in the Shared Public Routers, pointing at the Dedicated Public ESG.

Customer A has configured the inbuilt NSX Distributed Firewall to help secure the servers. It is entirely up to Customer A to determine whether this level of security is sufficient for their needs or further measures are necessary or advisable. For example, Customer A could supplement the NSX DFW with a third-party, VM-based next generation firewall (NGFW) appliance to implement more advanced security functions. A third-party cloud-based service might be another option. Telstra offers a number of comprehensive security solutions that may satisfy this requirement, some of which deploy logical security appliances while others are cloud-based.

In order to build this topology, Customer A will:

- Use the vSphere Telstra Plug-in to request a /29 public IP address range
- Configure a pair of VMs to act as the publicly reachable application servers and assign one of the public addresses to each of them
- Suitably configure the NSX Distributed Firewall
- Configure one of the public reachable addresses on Customer A’s Dedicated Public ESG. This address will be the default gateway for the servers
- Configure any other security or applications necessary to achieve Customer A’s objectives for the vDC.

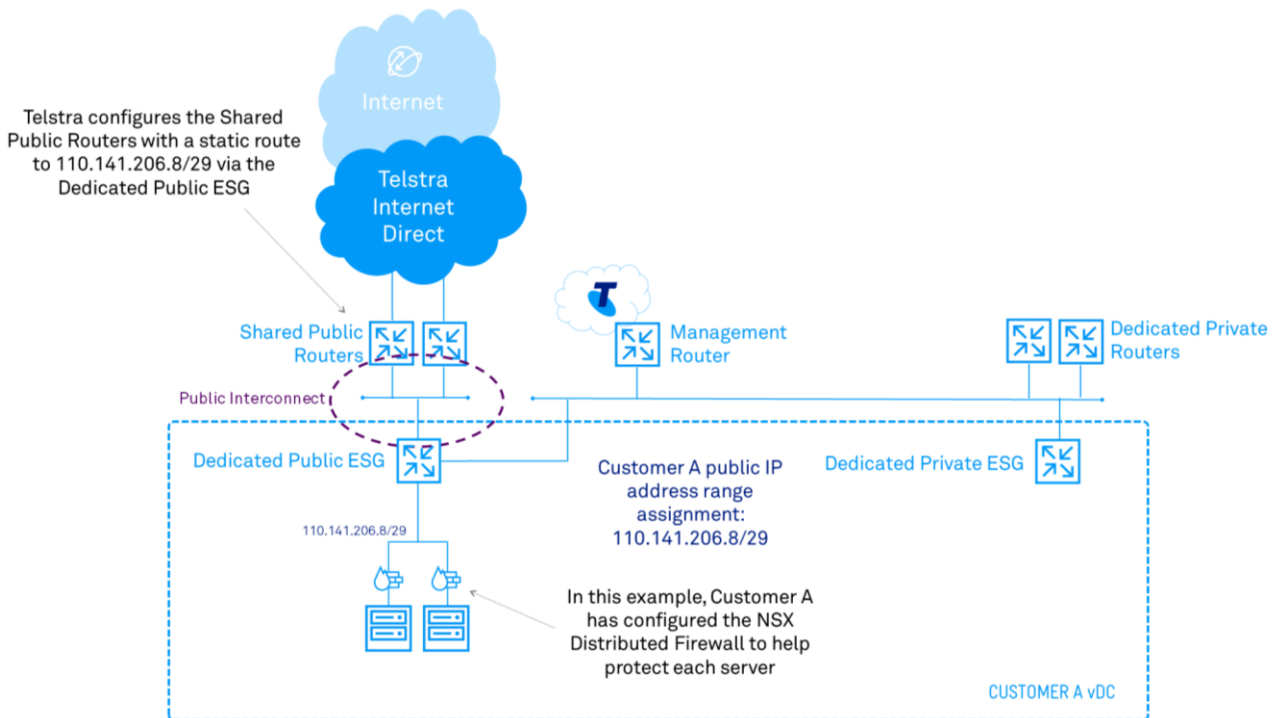


Figure 10: Basic Public Topology

PRIVATE

Most basic private topologies will exclusively use addresses from the RFC 1918 private ranges but this is not their defining characteristic. Rather, a basic private topology is one that exclusively communicates with external parties over the Private Interconnect.

You are responsible for providing all addresses you employ in a basic private topology. You must ensure they are compatible with your wider private network, and you decide which ranges are advertised to Cloud Gateway or your Next IP VPN.

If you try to use a public range you did not obtain through the vSphere Plug-in, you must remember that while you can communicate with addresses from that range over the *Private* Interconnect, it will not subsequently work with a *Public* Interconnect. All addresses used with the Public Interconnect must be obtained from Virtual Server (Dedicated) Gen1/Gen2/Gen2+.

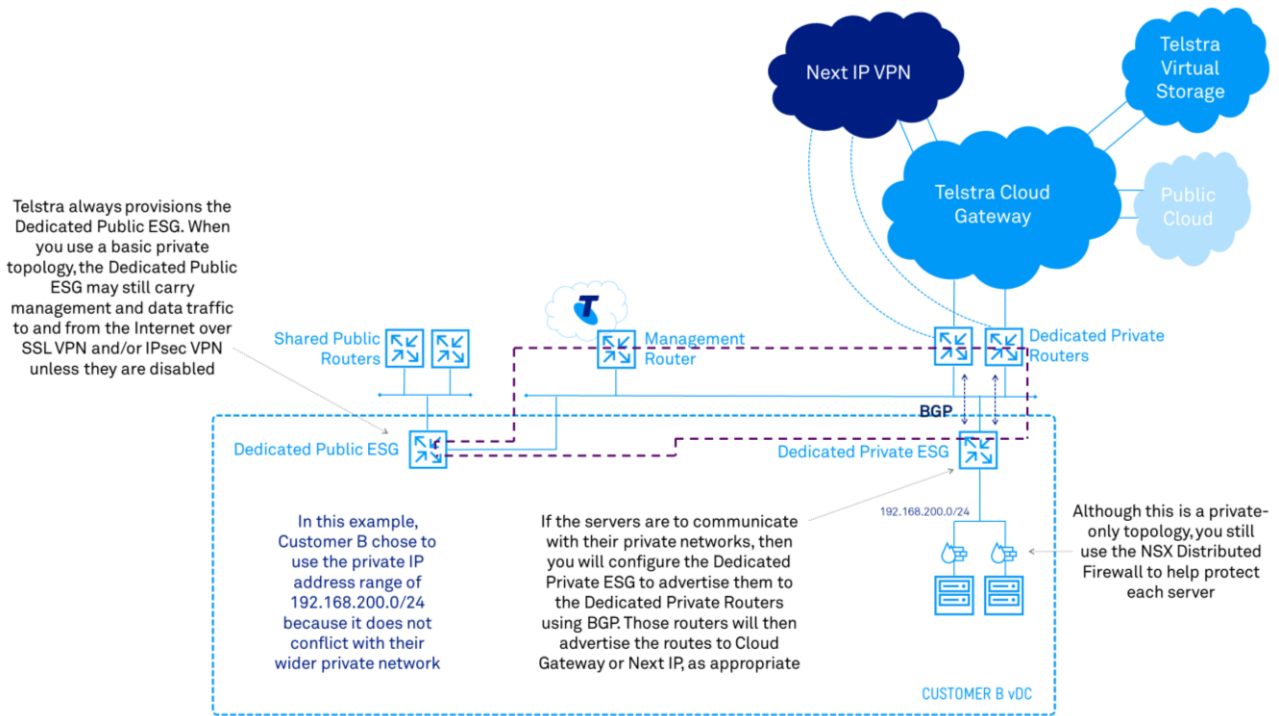


Figure 11: Basic Private Topology

EXTERNAL ACCESS TO PRIVATE TOPOLOGIES VIA VPN TUNNELS

Some customers that do not have a Next IP VPN or Cloud Gateway may use external private management and/or data access via SSL and/or IPsec VPN. This traffic still enters and leaves the vDC over the Private Interconnect but reaches the outside world via means other than Next IP or Cloud Gateway. This example is not the equivalent of a public topology because the servers still communicate through the Dedicated Private ESG as their first hop, and because they do not use IP addresses that can route natively through the Public Interconnect.

The location of the logical tunnel concentrator depends on who built it: Telstra (pre-uplift) or you (post-uplift)?

Prior to Virtual Server (Dedicated) Gen2+, Telstra built all logical VPN concentrators when we provisioned the vDC (SSL VPN) or the customer requested one (IPsec). Customers could not see the concentrators, nor change their configurations. When we uplift your vDC to Virtual Server (Dedicated) Gen2+, we leave any existing logical VPN concentrator(s) in place. They will still work as before and your VPN users will reach them at the same respective public IP addresses. However, you cannot see these concentrators and we will no longer make complex configuration changes to them. We discuss this rule in Task #SR07: Modify IPsec on page 83.

Beginning with Virtual Server (Dedicated) Gen2+, all new VPN concentrators sit on the Dedicated Public ESG. This is partly because NSX offers superior VPN features and capabilities to our legacy systems. There are two ramifications on your uplifted vDC:

1. At any time, you may decide to build a replacement IPsec and/or SSL VPN concentrator on your Dedicated Public ESG to exploit the capabilities of NSX
2. If you need to make a complex change to the configuration of either type of legacy VPN concentrator after we uplift your vDC, you will use NSX to create a new one on your Dedicated Public ESG and then configure it with the settings you need.

We define a 'complex' change as:

- For SSL VPN, anything other than a user ID or password change
- For IPsec VPN, anything other than modifying the Peer IP address of your IPsec client. The Peer IP address is the public IP address from which we expect your site concentrator to establish IPsec tunnels into Virtual Server (Dedicated).

In Figure 12, we show an example topology for 'Customer C', who does not have a Next IP VPN or Cloud Gateway connection. After uplift, Customer C decided to replace the old VPN concentrators and has configured a new one on the Dedicated Public ESG. Now, Customer C's users reach the basic private topology using an SSL or IPsec VPN that terminates on the Dedicated Public ESG and passes traffic across the Private Interconnect. Customer C also configured static routes in each ESG to allow traffic to pass successfully between the VPN tunnel and the private topology.

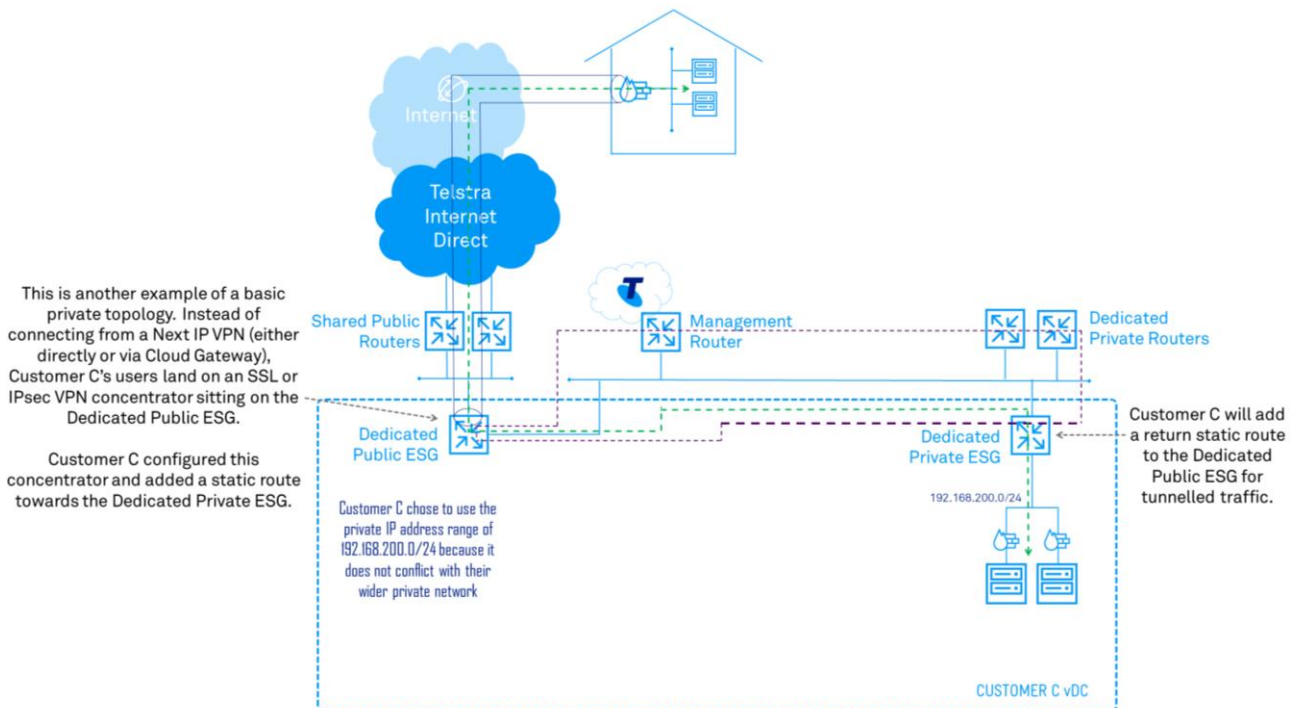


Figure 12: SSL VPN and IPsec VPN Access to a Basic Private Topology

COMPLEX TOPOLOGIES

You might need to use an advanced design in your vDC, involving public and private access to various parts of the topology but in a secure and controlled fashion. That is, some servers and other resources are visible to the Public Interconnect and some are visible to the Private Interconnect. Moreover, certain servers or resources might be visible to both, but via different interfaces and paths.

If you already used a complex vDC topology prior to uplift, it will remain in place after uplift and should work as before. However, you will now have more direct control over the topology and can make significant changes without involving us.

We show an example of a complex topology for 'Customer D' in Figure 13. In it, Customer D has divided the publicly visible topology into multiple logical segments using tiers and zones. Customer D has:

- Defined logical switches to build segments to arrange VMs and other resources in common zones and tiers
- Extensively used the NSX DFW on VM interfaces to apply stateful firewall rules locally on every server
- Added an ESG to load balance traffic to certain servers

- Implemented further VMs running third-party NGFW software for advanced security to protect the vDC as traffic enters from the Public Interconnect, and to separate and control communication between that area of the vDC and the rest of the customer's private networks.

Regardless of the design you choose to build into a complex topology, always remember that:

- Telstra must assign all public IP addresses that can be reached in your vDC through the Public Interconnect. If you use addresses in your public network topology that we did not assign to you, the Shared Public Routers will not be able to route traffic to them
- It is up to you to construct a topology that can successfully and securely communicate between:
 - Your Dedicated Public ESG and the VMs that are visible to the Internet
 - Your Dedicated Private ESG and the VMs the are visible to your private networks
 - VMs that need to be able to reach each other
- You remain responsible for the logical security of your vDC. This includes the configuration of appropriate rules within the NSX Distributed Firewall as well as additional security necessary to protect your vDC and any downstream systems and networks.

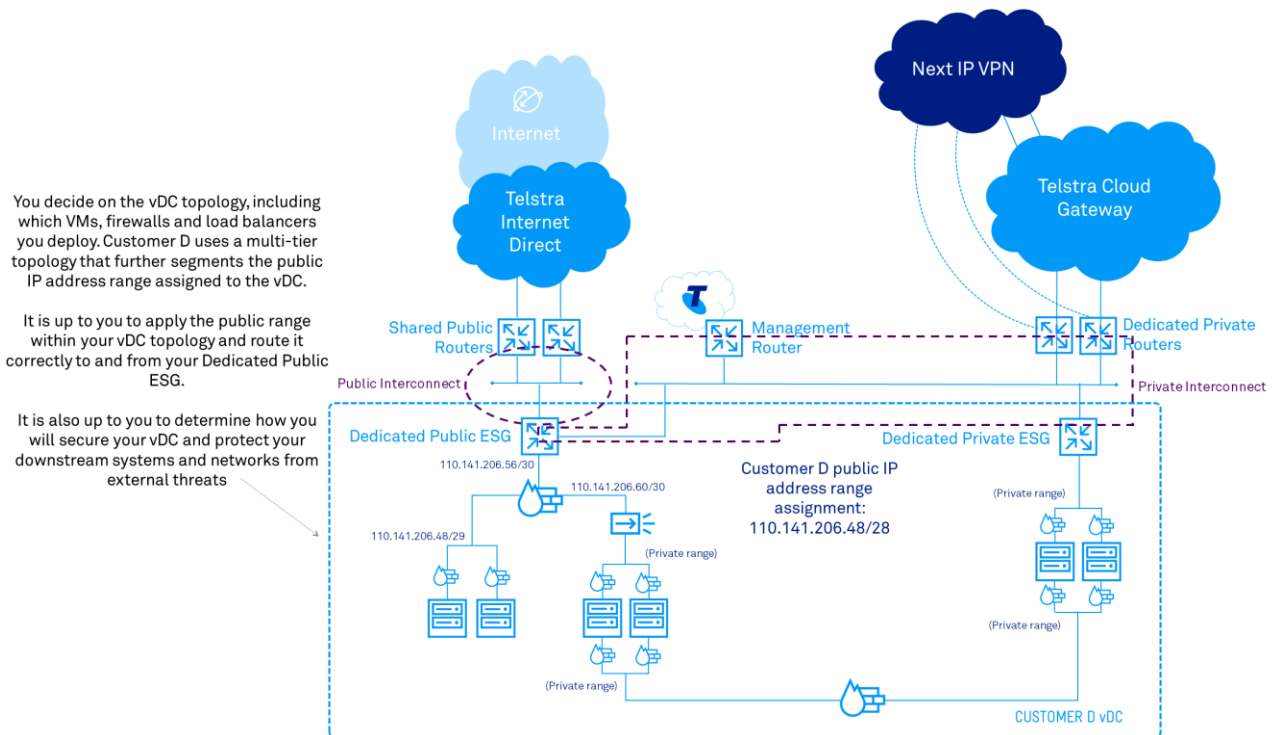


Figure 13: Example of Complex Network Topology and Addressing

Chapter 8

UPLIFT CONSIDERATIONS

NSX FIREWALL

Virtual Server (Dedicated) Gen1 employed a Cisco Virtual Security Gateway (VSG) for interface-level stateful firewall inspection (SFI) of traffic entering and leaving each VM in a vDC. Virtual Server (Dedicated) Gen2 used the NSX Firewall instead of the VSG. Virtual Server (Dedicated) Gen2+ exclusively uses the NSX Firewall.

When Telstra uplifts your vDC to Virtual Server (Dedicated) Gen2+, the method we use to migrate your logical firewall and its policy rules depends on which product you originally purchased. Refer to Table 9 for a summary of the effects of the uplift.

ORIGINAL PRODUCT	UPLIFT OUTCOME FOR LOGICAL FIREWALL AND RULES IN YOUR VDC
VIRTUAL SERVER (DEDICATED) GEN1	Telstra will replace your VSG with an NSX Firewall using a conversion process that exports your existing rules from the VSG and imports them to the NSX Firewall. After uplift, you will be able to see and control your NSX Firewall, including its rules and security groups
VIRTUAL SERVER (DEDICATED) GEN2	You already use the NSX Firewall. We will largely retain your existing configuration, only altering rules related to vDC management permissions. After uplift, you will be able to see and control your NSX Firewall, including all of its rules and security groups

Table 9: Uplift Outcomes for Logical Firewall and Rules in Your vDC

Your new NSX permissions are quite powerful because once we uplift your vDC, you will have administrative access to your NSX Firewall. You will be able to add new rules and change or delete existing rules for any of your vDC networks and devices. While this means you can be self-sufficient and configure your own firewall rules, it also means you assume a significant responsibility for the active security of your vDC and must be extremely careful to avoid accidental holes or blockages through misconfigurations and rule conflicts.

WHAT IS THE NSX FIREWALL?

The NSX Firewall provides logical security mechanisms for your vDC. It broadly categorises its policy application into two parts:

- Security between workloads and applications: known as the *Distributed Firewall* (DFW), this deals with 'east-west' SFI security. Conceptually there is only one DFW in each tenancy, which we automatically enable for you in every host cluster during provisioning. Because it runs in a distributed fashion in each hypervisor's kernel, the DFW will intelligently apply your security policy at an interface level on every VM in your vDC
- Perimeter security: known as an *Edge Firewall*, this refers to 'north-south' security that brings NAT, IPsec and SSL VPN along with SFI. Since an Edge Firewall may run in every ESG in your vDC, you can have as many Edge Firewalls as there are ESGs.

The vSphere NSX client will present your rules in a consolidated view shown in the order of application. You determine where to apply each rule (DFW or Edge Firewall, or both) along with its precedence when you define or modify it in vSphere.

Within this guide, we will typically use the term *NSX Firewall* to cover both firewall types unless we need to discuss a specific or unique characteristic of one or the other.

POST-UPLIFT VIEW

Telstra uses a consistent approach to the configuration of each customer's NSX Firewall. That approach harnesses several capabilities inherent to NSX that help to organise policies and rules. These capabilities were important to the Cloud Services Management Console (CSMC) because it allowed customers of Virtual Server (Dedicated) Gen2 to define their own rules and have them added to the NSX Firewall using backend automation.

At a high level, the NSX Firewall can arrange firewall policy rules into *sections*. A section is analogous to an administrative grouping of rules that make them easier to read and comprehend. Some sections are automatically appended by NSX, but we have added most of those you will see when you first log into vSphere after uplift.

Table 10 shows our use of sections to organise the NSX Firewall for your vDC. They occur sequentially in the order we show them here, as do their rules.






SECTION NAME	CREATOR	PURPOSE
PRI_CUSTOM		Holds firewall rules applied to your private networks. You will have specified these rules either manually (Gen1) or using the CSMC (Gen2)
PUB_CUSTOM		Holds firewall rules applied to your public networks. You will have specified these rules either manually (Gen1) or using the CSMC (Gen2)
PRI_DEFAULT		Catch-all permit rule applied to your private networks
PUB_DEFAULT		Catch-all deny rule applied to your public networks
DEFAULT SECTION LAYER3		Contains assorted default rules that will only apply if no matches occur to the rules in the preceding sections

Table 10: NSX Firewall - Section Organisation Post-Uplift

Once uplifted, you are free to re-arrange the NSX Firewall as you see fit. You may add, modify or delete any section and add, modify, delete, disable or enable any rules.

ESG: DEFAULT FIREWALL TRAFFIC POLICY RULE

When you create an NSX ESG using the inbuilt wizard, you will have the opportunity to enable its default firewall rule. The default firewall rule is a very simple catch-all for any traffic flowing through the ESG that does not match a customised firewall rule configured in the NSX Firewall administration panel. It only has two states:

1. Deny all traffic
2. Allow all traffic.

In an example of the differences in capabilities between them, the default firewall traffic policy rule does not appear in the vSphere HTML5 client but does appear in the Flex client. This may initially confuse the administrator, particularly if the effects of the default rule contradict expected behaviour.

When Telstra configures your Dedicated Public ESG and Dedicated Private ESG during original provisioning or as part of our uplift process, we will apply a default traffic policy that allows all traffic. You can see or change this rule using the Flex client.

SECURITY GROUPS

You can arrange administrative objects in the NSX Firewall in a number of flexible and powerful ways. For example, you can construct atomic objects into *groups* and then apply a single rule to the whole group at once. The atomic objects can consist of all sorts of resources including VMs, IP addresses or entire ranges, logical switches, vApps, or even a whole host cluster or vDC. One group can also be a member of another group so you can build a nested hierarchy of objects ranging from the broad to the specific.

Consider this simple scenario, which is somewhat representative of Telstra's approach:

- You add all logical switches deemed to be 'private' networks to a Private Networks security group
- You then apply a policy rule to your Private Networks group. This rule automatically captures any VM interface connected to any of the logical switches in the Private Networks group, including those added subsequent to the rule definition.

Telstra used security groups in Virtual Server (Dedicated) Gen2 to help us administer and organise firewall rules for public and private networks in customers' vDCs. When you assume control of your NSX Firewall, you will be able to see those groups and add, change or delete them.

PRIVATE VIRTUAL MACHINES

Virtual Server (Dedicated) Gen1 used customer-specific VLANs from the Dedicated Private Routers to connect private VMs. If a customer had multiple private VMs, they could share a single VLAN or spread over multiple VLANs as needed.

Each VLAN was called a 'Private Network'. After a customer ordered a Private Network and supplied an appropriate private IP subnet, Telstra would select and configure a VLAN and extend it to the vDC. Telstra would also consume the first few usable addresses in the subnet to build a redundant default gateway on the Dedicated Private Routers. The customer could attach VMs to the segment in the vDC and assign them IP addresses in the same subnet.

Telstra will not touch any of these VLAN-based Private Networks when we uplift a vDC from Virtual Server (Dedicated) Gen1. However, you will not have any increased control over them, because you will not have any administrative access to the Dedicated Private Routers or the intermediate switching infrastructure.

If you are a Virtual Server (Dedicated) Gen1 customer and use any Private Networks, Telstra encourages you to migrate them to NSX-based ESGs and/or logical switches so you can configure and manage them yourself. But you will not be able to do so without our assistance because we must re-arrange routing in the Dedicated Private Routers to allow traffic to reach your new NSX-based segment over the Private Interconnect. To begin the process, you can submit a special request to us using our vSphere Plug-in.

We show an example of the treatment of Private Networks in Figure 14.

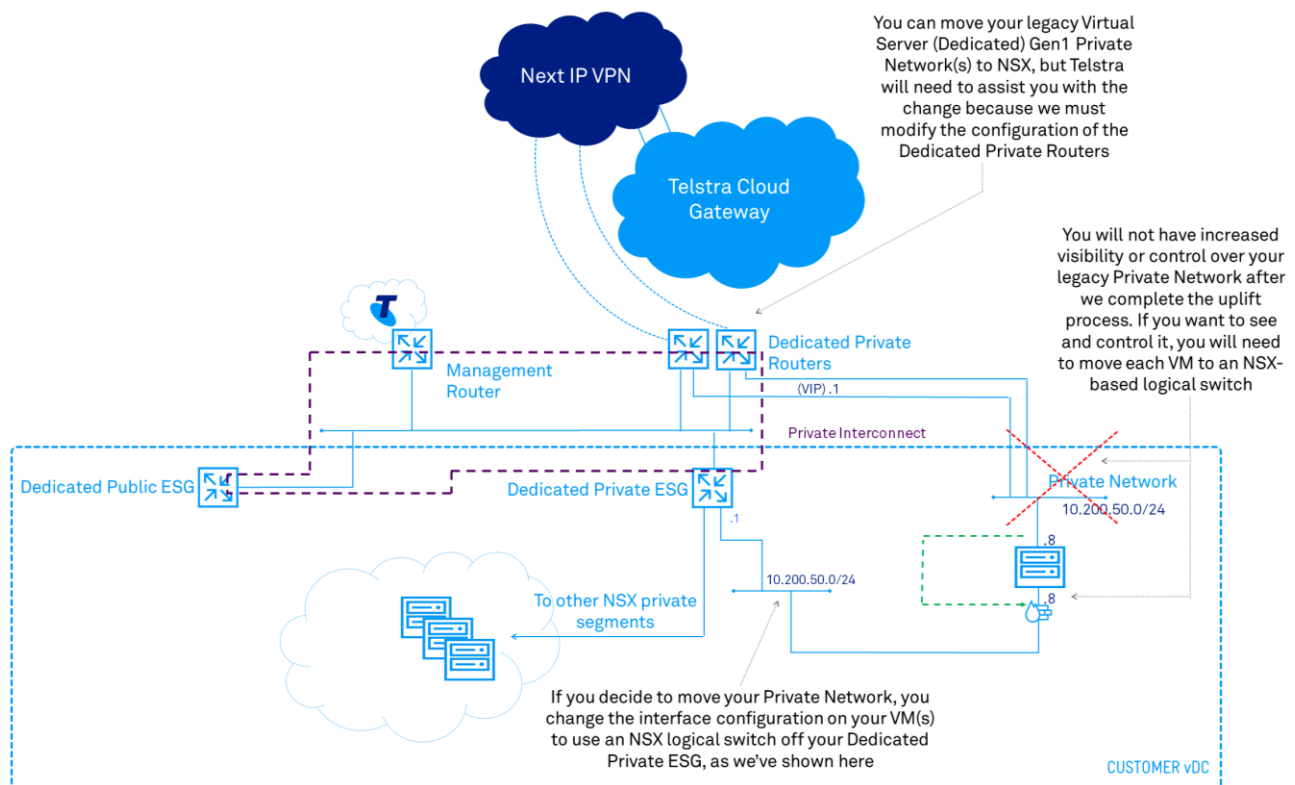


Figure 14: Treatment of Virtual Server (Dedicated) Gen1 Private Networks During Uplift

SHARED PUBLIC NETWORK MIGRATION

Both Virtual Server (Dedicated) Gen1 and Gen2 used a 'Shared Public Network' for Internet access to and from each vDC. The Shared Public Network was a logical segment that contained VMs from numerous customers. Telstra assigned the specific public address to each VM attached to the Shared Public Network. We locked the assigned IP address to a particular VM interface MAC address to prevent spoofing attacks. Each customer could request up to five shared public IP addresses and would specify the respective interface MAC address for the VM when ordering one.

Since the Shared Public Network contained VMs from numerous customers and Telstra assigned addresses on a first-come, first-served basis, addresses would often appear non-contiguous to a single customer with multiple VMs. And because it was considered part of 'the Internet', the shared public network could carry traffic between the public interfaces of VMs from all customers. Customers would then specify their own customised firewall rules to protect their VMs.

When we uplift your vDC, we want each VM from the Shared Public Network to continue to function seamlessly. However, we need to 'move' your VMs from the Shared Public Network onto a dedicated segment that we build for you in your vDC.

After uplift, you will see in your vDC one or more new dedicated segments with public IP addresses. These segments are specific to you but will each re-use the subnet range employed in the Shared Public Network. We will also re-use the original default gateway address on your Dedicated Public ESG during the uplift process, allowing your VM(s) to communicate with the outside world without requiring an addressing change.

We will manipulate the routing of traffic to and from your vDC to allow this arrangement to work. You are not free to use any other addresses in the same subnet, even those that otherwise fit within the subnet mask. This is because the Shared Public Routers use a host route to your vDC for each specific address and will not forward traffic for other addresses to your vDC unless we have assigned them to you.

We show an example of our migration approach for the Shared Public Network in Figure 15.

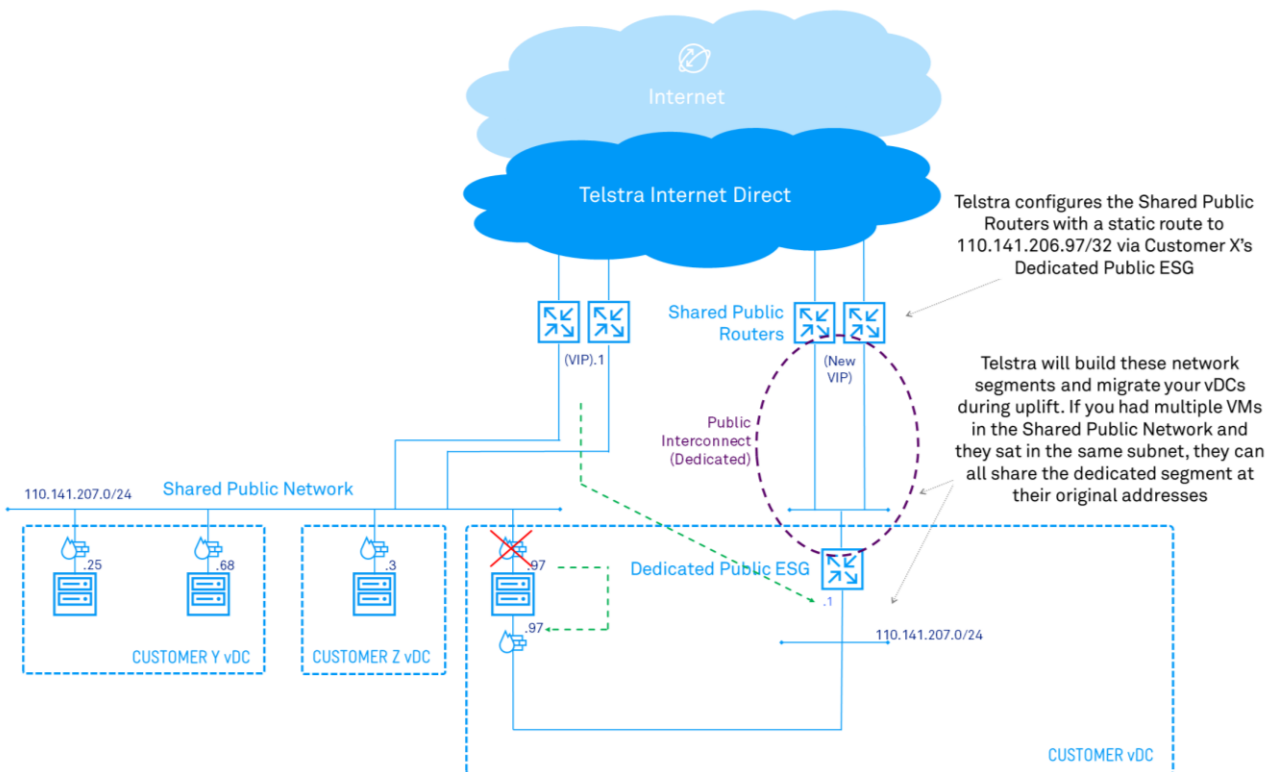


Figure 15: Shared Public Network Migration During Uplift

LOAD BALANCERS

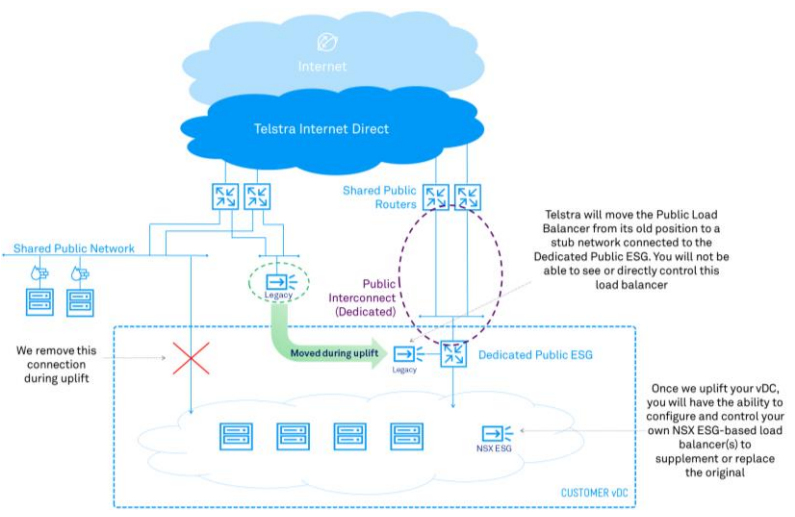
Virtual Server (Dedicated) Gen1 offered load balancers for VMs reached over public or private interconnections. We consider these load balancers to be legacy models. Virtual Server (Dedicated) Gen2 also offered load balancers for VMs reached over public or private interconnections but used NSX ESG-based virtual devices instead of the equipment from Gen1.

Telstra’s names for each load balancer reflected its position and job:

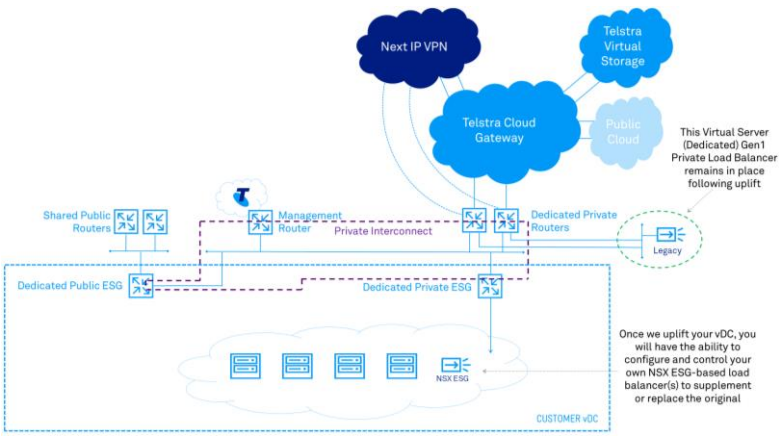
- a. For VMs reached over the Shared Public Network: **Public Load Balancer**
- b. For VMs reached from Next IP and/or Cloud Gateway: **Private Load Balancer**.

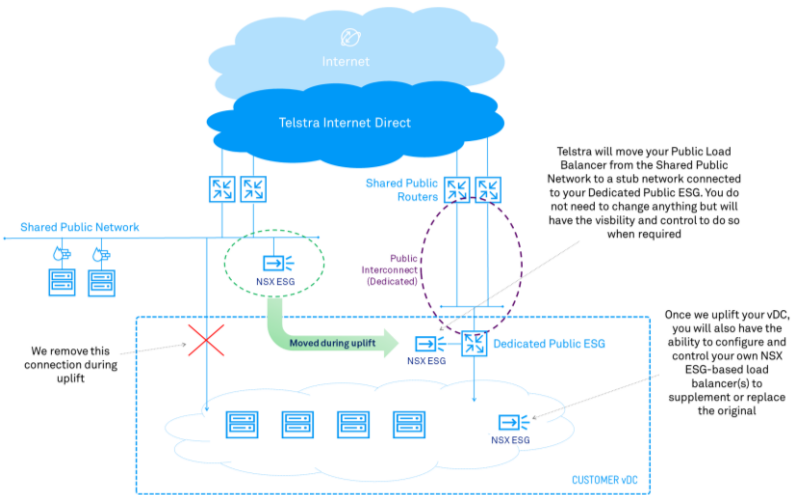
In all cases, Telstra would configure a load balancer with settings nominated by our customers.

Following uplift, the existing load balancers will remain in place, but their ongoing lifecycle management and configuration varies according to their type. We cover uplift outcomes and your options for future load balancers in Table 11.

UPLIFTED FROM	LEGACY LOAD BALANCER TYPE	UPLIFT OUTCOME AND OPTIONS
<p>VIRTUAL SERVER (DEDICATED) GEN1</p>	<p>LEGACY PUBLIC LOAD BALANCER</p>	<p>Telstra will move and re-attach the load balancer as a stub off the side of the Dedicated Public ESG. You will not be able to directly control this load balancer and future support will be limited.</p> <p>Telstra encourages you to supplement or replace it with one or more NSX ESG-based load balancers you configure and control using the vSphere client.</p> 

UPLIFTED FROM	LEGACY LOAD BALANCER TYPE	UPLIFT OUTCOME AND OPTIONS
---------------	---------------------------	----------------------------

	<p>LEGACY PRIVATE LOAD BALANCER</p>	<p>Remains in place as a stub off the side of the Dedicated Private Routers. You will not be able to see or directly control this load balancer and future support will be limited.</p> <p>Telstra encourages you to supplement or replace it with one or more NSX ESG-based load balancers you configure and control using the vSphere client.</p>  <p>Once we uplift your vDC, you will have the ability to configure and control your own NSX ESG-based load balancer(s) to supplement or replace the original</p>
--	--	--

<p>VIRTUAL SERVER (DEDICATED) GEN2</p>	<p>NSX ESG-BASED PUBLIC LOAD BALANCER</p>	<p>Telstra will move and re-attach the load balancer as a stub off the side of the Dedicated Public ESG.</p> <p>You will assume control of this load balancer through the vSphere client.</p>  <p>Telstra will move your Public Load Balancer from the Shared Public Network to a stub network connected to your Dedicated Public ESG. You do not need to change anything but will have the visibility and control to do so when required</p> <p>Once we uplift your vDC, you will also have the ability to configure and control your own NSX ESG-based load balancer(s) to supplement or replace the original</p>
---	--	---

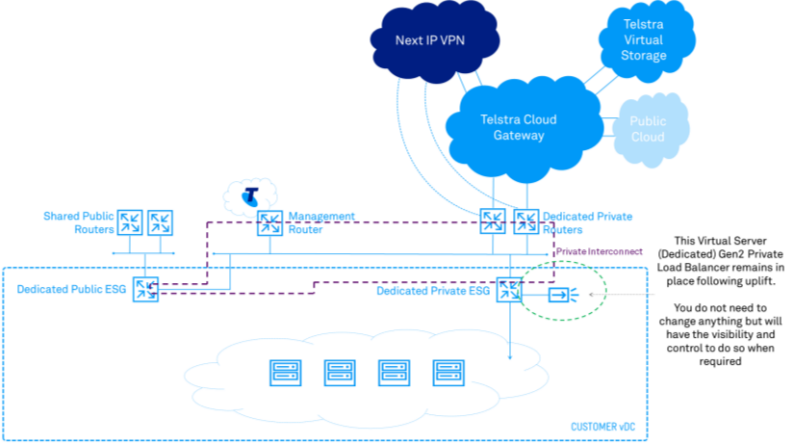
UPLIFTED FROM	LEGACY LOAD BALANCER TYPE	UPLIFT OUTCOME AND OPTIONS
	NSX ESG-BASED PRIVATE LOAD BALANCER	<p>Remains in place.</p> <p>You will assume control of this load balancer through the vSphere client.</p> 

Table 11: Uplift Outcomes for Load Balancers

If we uplifted you from Virtual Server (Dedicated) Gen1 or you did not use load balancers in your vDC prior to uplift, you may subsequently decide to implement an NSX ESG-based version yourself. If so, you face a choice about where to put it.

When Telstra built an NSX ESG-based Public or Private load balancer for our Virtual Server (Dedicated) Gen2 customers in the past, our policy was to commission each in an ESG built for that purpose on a host running in the customer’s vDC. You may choose to do the same (build an ESG for this purpose) but you may equally decide to implement it in one of the default ESGs (Dedicated Public or Dedicated Private, as appropriate) instead. That is your choice, but you will need to consider the resource impacts on the underlying VM hosting the ESG as well as the risks of misconfiguration, which could harm your vDC’s external connectivity.

DRS AFFINITY RULES

The Distributed Resource Scheduler is a utility that can allocate and migrate workloads across physical resource pools to improve processing efficiency and support maintenance. For example, it can automatically balance VMs across hosts according to their resource demands. It can also constrain the way that VMware’s HA feature shifts affected VMs when a host fails.

Default DRS behaviour may suit simple implementations but sometimes you may have more sophisticated needs, such as ensuring the ongoing co-location or separation of certain workloads. VMware allows the creation of rules to meet these needs using *DRS Affinity*.

DRS Affinity influences the automated operation of DRS and how it allocates VMs across the available hosts in a DRS cluster through affinity **rules**. There are two types of rules:

- a. VM-Host: specify affinity or anti-affinity between VMs and hosts in a cluster. This type of rule works on groups of VMs (*VM Groups*) and hosts (*Host Groups*). You must define both groups before you can use them in a VM-Host affinity or anti-affinity rule
- b. VM-VM: specify affinity or anti-affinity between individual VMs in a cluster. You select the VMs involved when you define the rule.

Affinity rules generally tie resources together so they are co-located, whereas *anti-affinity* rules separate them. For example, a VM-Host affinity rule is intended to run a group of VMs on a particular group of hosts. On the other hand, a corresponding VM-Host anti-affinity rule would attempt to keep the VMs away from the group of hosts.

When you define or change a VM-Host affinity or anti-affinity rule, you can categorise it as either *required* (equivalent to 'must') or *preferential* ('should'). The difference is important, because DRS sometimes need discretion so that during a failure it can permit HA to migrate a workload to a host that would otherwise be disallowed. In other words, a preferential rule might allow HA to temporarily move a workload to a location that a mandatory rule would not, keeping the workload functioning rather than letting it fail.

Under normal circumstances, DRS will attempt to honour all your affinity rules as it distributes VMs across a cluster of hosts. When DRS cannot fulfil the affinity conditions because it has no discretion, certain rules conflict, or there is a lack of available resources, it is called an *affinity violation*. vSphere reports affinity violations and the reason(s) they have occurred under 'Faults' in the DRS monitoring panel.

PRE-UPLIFT VIEW

Telstra did not give you sufficient permissions to control DRS Affinity in Virtual Server (Dedicated) Gen1 or the initial release of Virtual Server (Dedicated) Gen2. Rather, you could manually request it from us. We subsequently released an enhancement to the CSMC that allowed you to submit your request in an online form. But in all cases, our Operations team completed the configuration of DRS Affinity to meet your specifications.

Our DRS Affinity support came with certain limitations intended to help protect your vDC from affinity violations and HA failures, and to allow us to perform background maintenance on your vDC equipment. There were two notable capabilities of DRS Affinity that we did not support:

- a. VM-Host anti-affinity
- b. VM-Host required ('must') affinity rules.

We also specified further conditions under which we would support DRS Affinity. In summary, they were:

- To use a VM-Host or VM-VM affinity rule, you required at least two hosts (then called 'blades') in the cluster
- To use a VM-VM anti-affinity rule, you required the greater of the following:
 - At least three hosts in the cluster, or
 - One more host than the number of VMs specified in the rule
- To use a VM-VM affinity or anti-affinity rule, you specified at least two VMs. While there was no stated upper limit on the number of VMs in a VM-VM anti-affinity rule, it would be constrained by the number of blades in the cluster.

POST-UPLIFT VIEW

When you first login after uplift, your pre-uplift DRS Affinity configuration will remain in place, but you will now have additional permissions to directly control it. This means you assume responsibility for DRS Affinity and may create rules that can cause rule conflicts or affinity violations. If that happens, it could complicate our ability to support you or perform background maintenance on your vDC.

So once uplift occurs, while you are free to implement DRS Affinity as you see fit, we recommend that you broadly follow our configuration recommendations for any future changes. These are mostly the same as they were pre-uplift, but are slightly more flexible:

- Continue to avoid VM-Host affinity or anti-affinity rules that are categorised as required (ie. 'must')

- If you plan to use a VM-Host anti-affinity rule, ensure your cluster contains at least one extra host with sufficient spare capacity to accept migrated workloads during failures.

Whether or not you employ sophisticated DRS affinity rules, we encourage you to carefully analyse them prior to commissioning to ensure you do not experience unexpected or unwanted side effects.

LAYER-2 STRETCH

A 'stretched' layer-2 data path connects one or more pairs of matched LAN segments over an intermediate layer-3 network. Within the VMware community, it is commonly called *Layer-2 Stretch*. Because each end of the stretched path can reside in a different physical site, Layer-2 Stretch may appeal to organisations that want to progressively migrate their processing from one location to another, or perhaps to replicate data between active and standby DCs. Layer-2 Stretch will work with either VLANs or VXLANs, both separately or co-operatively.

Security is an important aspect of Layer-2 Stretch because some or all of the intermediate layer-3 network may be public (eg. the Internet) or otherwise untrusted. As a result, it uses an NSX feature called *L2 VPN* consisting of co-operating endpoints that tunnel data through SSL or IPsec. Each tunnel endpoint resides in an ESG.²

Once we uplift your vDC to Virtual Server (Dedicated) Gen2+, you will have the ability to build your own Layer-2 Stretch service. VMware produces a set of best-practice guidelines to help you design your Layer-2 Stretch service if you decide to build one.

Telstra strongly recommends you familiarise yourself with the characteristics and capabilities of Layer-2 Stretch and L2 VPN to ensure your tunnel(s) is secure and you do not accidentally create loops and duplicate packets.

² At the time of writing, the administration of L2 VPN is somewhat inconsistent:

- You cannot administer any L2 VPN endpoint using the vSphere HTML5 client
- You can administer the SSL-capable L2 VPN endpoint using the Flex client
- If you want to use the IPsec-capable L2 VPN endpoint, you must configure it using the vSphere REST API

Chapter 9

USING AN EMAIL SERVER IN CSX GEN2+

OVERVIEW

All outbound email traffic emanating from your Virtual Server (Dedicated) Gen2+ vDC over the Public Interconnect must pass through our inbuilt SMTP mail relay or an approved external product. We apply SMTP controls upstream of your Dedicated Public ESG to enforce this rule, which has existed for all generations of our Virtual Server (Dedicated) product.

When we uplift your vDC to Virtual Server (Dedicated) Gen2+ we will not alter your settings for any existing mail relay service(s), whether inbuilt or external.

REQUEST AN SMTP MAIL RELAY FROM TELSTRA

You can request an inbuilt SMTP mail relay using the vSphere Plug-in. You will incur charges for this service. When you order the SMTP mail relay using the Plug-in, you will also need to tell us each domain name for which we will relay email.

After you submit the request, we email the mail server set-up details back to you. You can then configure your mail server software accordingly.

All emails you send to the inbuilt SMTP mail relay must use one of the domain names you specified in the setup process, in the **from** field of the email. Using any other domain name will cause our filters to reject the email.

APPROVED EXTERNAL PRODUCTS

We allow you to use any of several alternatives to our inbuilt SMTP mail relay. We support:

- a. Microsoft Office 365
- b. Symantec.Cloud
- c. Telstra Internet Protection Mail.

Telstra Internet Protection Mail is available for purchase from us. If you wish to use Microsoft Office 365 or Symantec.Cloud, you may buy these services from Telstra or through another channel. Contact your account team or a Telstra partner for more information.

SUPPORTED PORT NUMBERS

If you use one of the approved external products, you must ensure you use supported port numbers for outgoing sessions. The following table shows the port numbers valid for each product. You should assume these port numbers refer to TCP unless advised otherwise by the product concerned.

PRODUCT	MICROSOFT OFFICE 365	SYMANTEC.CLOUD	INTERNET PROTECTION MAIL
PORTS	25, 465, 587	25	25

Chapter 10

JOB EXAMPLES

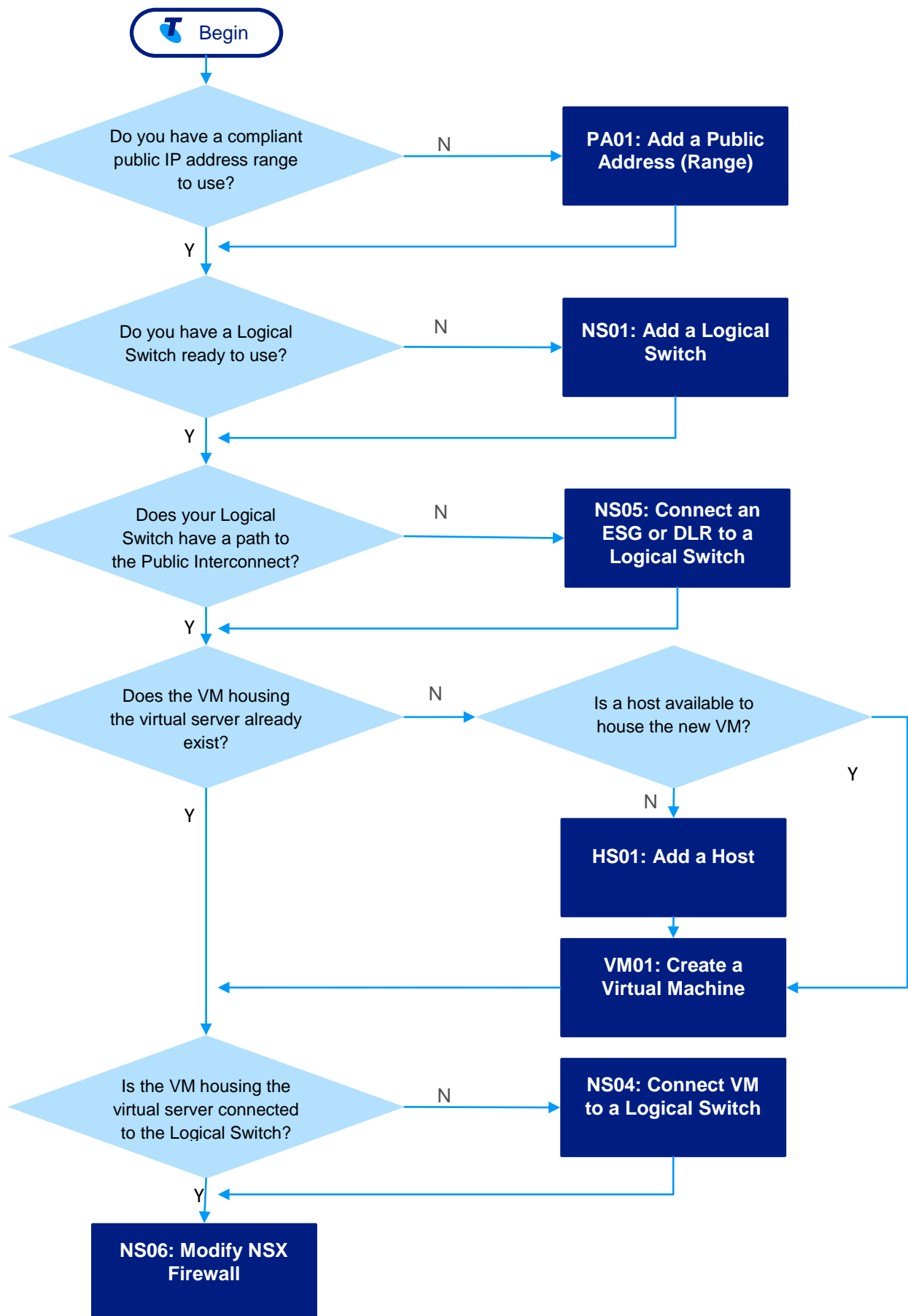
OVERVIEW OF JOBS

In this chapter, we explore examples of jobs you might undertake while managing your vDC. We have structured them according to the common tasks you will execute as you complete the job. Some consist of several tasks and others are more straightforward.

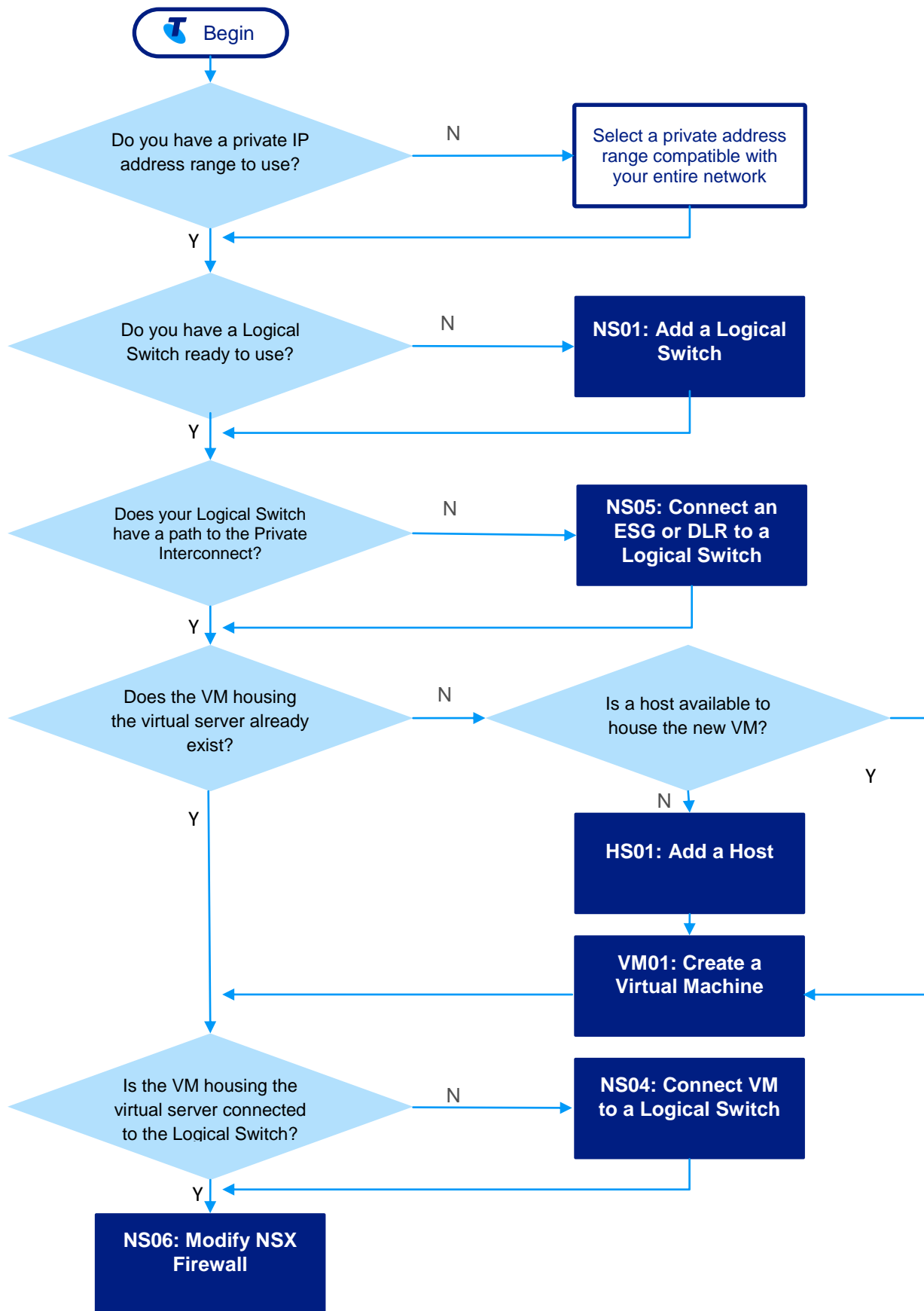
As you review a job, keep in mind the following points:

- 1 Some tasks in the job may be optional or not required. We will generally include questions that prompt you to decide whether you need to complete each task
- 2 Tasks that involve the Telstra Plug-in often have an SLA of several days, although Telstra regularly fulfils plug-in tasks in a much shorter time. If your job includes a number of plug-in tasks, where possible you might consider submitting them in parallel to compress the elapsed time your job will take to finish
- 3 It is very important to be fully briefed on vCenter and NSX so that you design and implement your solutions efficiently and securely. We provide you with a number of hyperlinks to VMware Docs to help you research your tasks beforehand, but it is not an exhaustive list. As you read VMware Docs, you will find much more information available to help you understand the task at hand
- 4 There may be tasks we do not cover in this guide because we do not commonly see them used in our customers' vDCs.

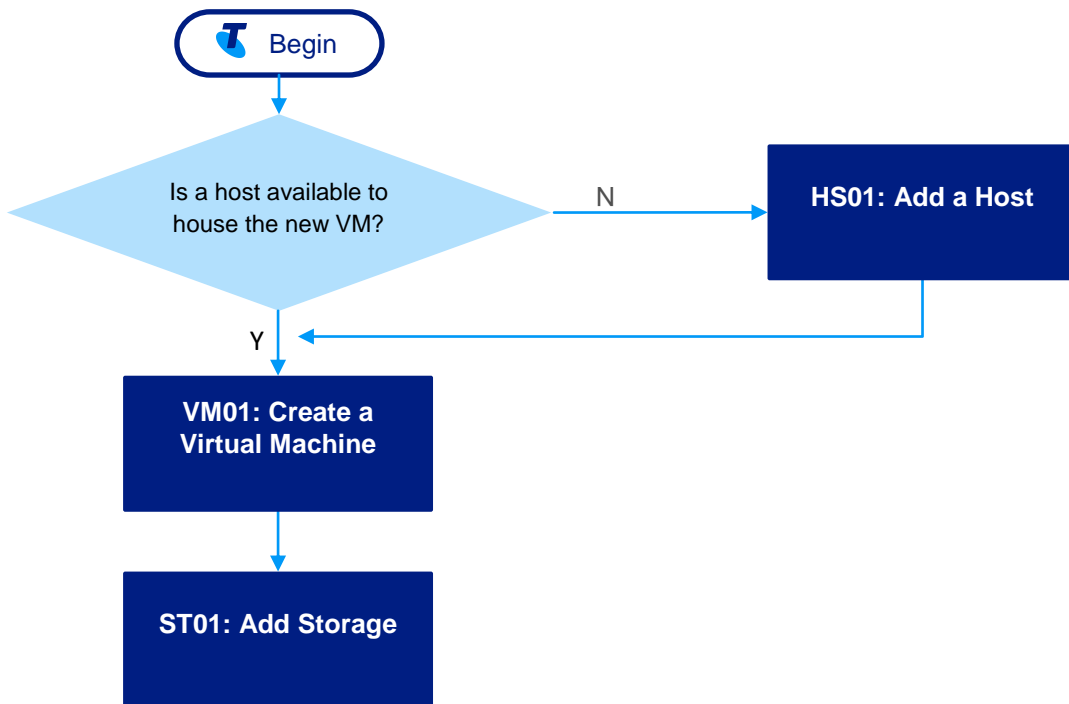
JOB #1: ADD A VIRTUAL SERVER TO A PUBLIC NETWORK



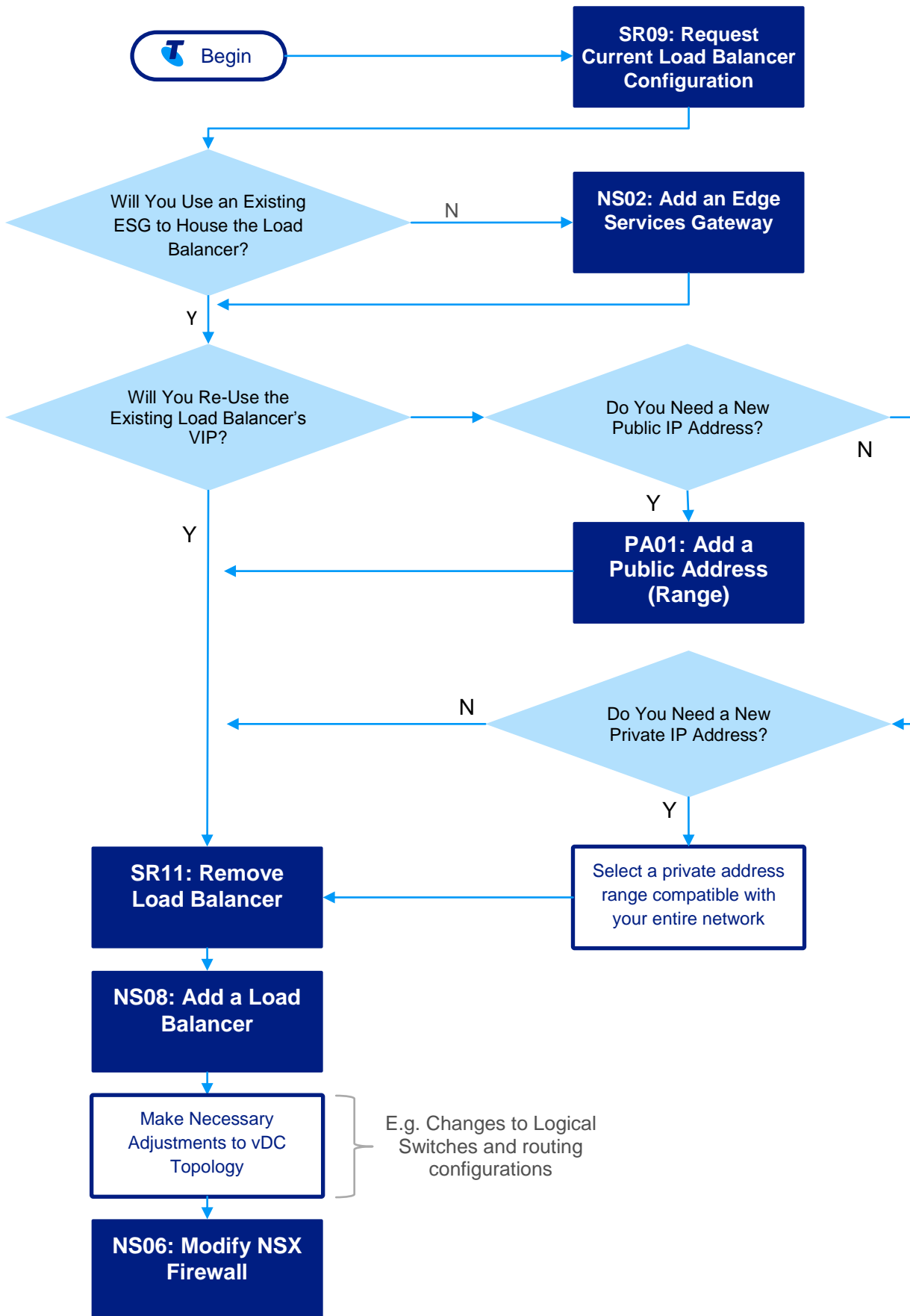
JOB #2: ADD A VIRTUAL SERVER TO A PRIVATE NETWORK



JOB #3: ADD A VIRTUAL SERVER WITH NEW STORAGE



JOB #4: REPLACE VIRTUAL SERVER (DEDICATED) GEN1 PUBLIC LOAD BALANCER



Chapter 11

HOST TASKS

TASK #HS01: ADD A HOST

SERVICE LEVEL AGREEMENT	REQUIRED USER TYPE:	APPLIES TO UPLIFT FROM:
<input type="checkbox"/> TELSTRA AUTOMATED	<input checked="" type="checkbox"/> ADMIN/2/3/4/5	<input checked="" type="checkbox"/> VIRTUAL SERVER (DEDICATED) GEN1
<input checked="" type="checkbox"/> MANUAL (SUBJECT TO SLA)	<input type="checkbox"/> NETWORKADMIN	<input checked="" type="checkbox"/> VIRTUAL SERVER (DEDICATED) GEN2
<input type="checkbox"/> CUSTOMER AUTOMATED	<input type="checkbox"/> READONLY	

OVERVIEW

A **host** is a physical server in a *Virtual Server (Dedicated) Gen2+* vDC. When you intend to add a host to your vDC, Telstra's VMware Plug-in will present a list of alternative host specifications from which you select your preference. The host specifications for each option will show:

- The family and model
- The number of CPUs and
- The amount of RAM.

The plug-in does not reveal the vendor of the underlying hardware. Telstra also plans to remove advice about the family and model of host in a future update.

It is up to you to decide whether the host specifications are suitable for your intended purpose. Telstra does not recommend or endorse any particular configuration for specific applications or workloads.

During provisioning, Telstra will install VMware ESXi onto the new host(s) and each will become visible in vCenter.

CLUSTERS

Virtual Server (Dedicated) Gen2+ arranges all hosts into **clusters**. Each cluster will contain between two and 16 hosts. Product rules stipulate that every host in a cluster must have the same hardware configuration (number of CPUs, number of cores per CPU and amount of RAM).

When you order one or more new hosts, you will select your preferred hardware configuration. If you already have a cluster containing hosts with those exact specifications, you are allowed to add the new host(s) to that cluster if you wish, provided you will not exceed the 16-host limit. If you plan to put the new hosts in a new cluster, you must order at least two of them.

Telstra assigns the cluster name when we provision it. You cannot change the name of the cluster. The format of the name is:

```
<DC Code>-<Service ID>-<Management Type>-clust<Sequence Number>
```

The following table describes each section of the name.

SECTION	MEANING	EXAMPLE(S)
DC CODE	The code representing the location of the DC housing your tenancy	Clayton, Vic: clay St Leonards, NSW: slen Gnangara, WA: gnan
SERVICE ID	A 7-digit number representing your compute tenancy	9620081
MANAGEMENT TYPE	The party responsible for managing the host	Self-managed: sm (Currently, this is the only supported option for Virtual Server (Dedicated) Gen2+)
SEQUENCE NUMBER	Each new cluster is numbered sequentially from 001	For the second cluster: Sequence Number: 002

The following example shows the name of the fourth cluster provisioned in tenancy N1625678R in Clayton, Victoria:

```
clay-1625678-sm-clust004
```

When we provision a new cluster for you, Telstra will configure or enable various attributes of DRS and HA to facilitate vMotion, but with certain restrictions. You can use vMotion and further modify the settings of DRS and HA within the limits we set. We recommend you only change settings to meet a specific need and that you fully consider the ramifications. If you incorrectly configure DRS and/or HA you may compromise your vDC's performance and availability.

HOST NAMES

Virtual Server (Dedicated) Gen2+ automatically assigns a name to each host when we provision it. The format of the name is:

```
<Service ID><DC Code><Hypervisor Type><Management Type><Sequence  
Number>.cust.cloud.telstra.com
```

The following table describes each section of the name.

SECTION	MEANING	EXAMPLE(S)
SERVICE ID	A 7-digit number representing your compute tenancy	1625678
DC CODE	The code representing the location of the DC housing your tenancy	Clayton, Vic: cl St Leonards, NSW: sl Gnangara, WA: gn
HYPERVISOR TYPE	The hypervisor loaded onto the host by Telstra's provisioning team	VMware ESXi: e (Currently, this is the only supported option for CSX GEN2+)

SECTION	MEANING	EXAMPLE(S)
MANAGEMENT TYPE	The party responsible for managing the host	Self-managed: sm (Currently, this is the only supported option for CSX GEN2+)
SEQUENCE NUMBER	Each new host in a cluster is numbered sequentially from 01	For the second host in the cluster: Sequence Number: 02

The following example shows the name of the fourth host provisioned in tenancy N1625678R in Clayton, Victoria:

```
1625678clesm04.cust.cloud.telstra.com
```

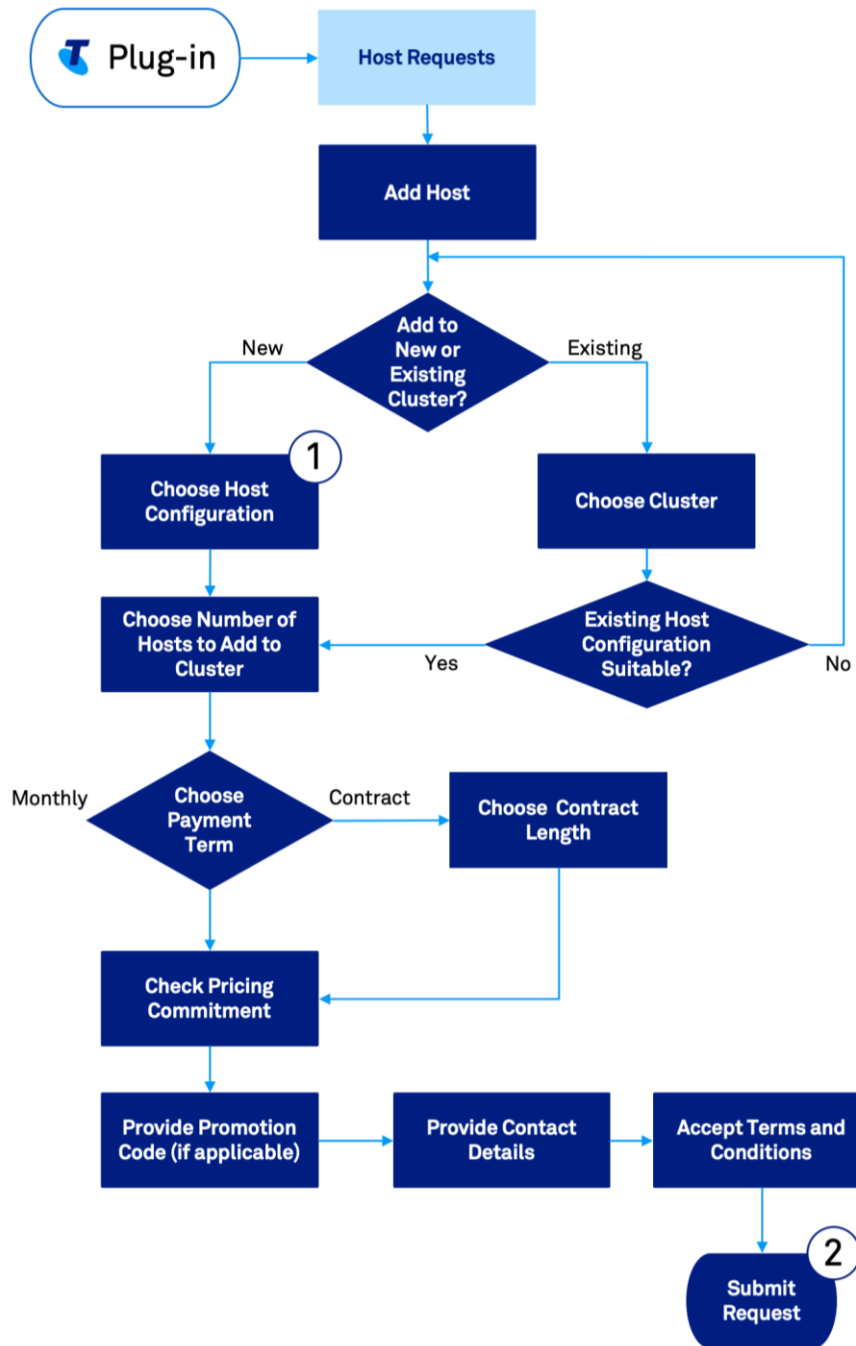
The vSphere client will present each host in a hierarchy grouped by cluster name. You cannot rename any host.

PREREQUISITES

Before you can submit a Host Request, you must:

1. Log into the vSphere Client for your vDC using one of your read-write administration accounts for vCenter.

PROCEDURE



NOTES

- 1 The host configurations you may choose from are:
 - a. B200 M4 Blade (2 CPU, 128GB RAM)
 - b. B200 M4 Blade (2 CPU, 256GB RAM)
- 2 After you submit your request, the plug-in will return a Request ID. In a future release of the plug-in, the Request ID will help you track and review your service history.

TASK #HS02: REMOVE A HOST

SERVICE LEVEL AGREEMENT	REQUIRED USER TYPE:	APPLIES TO UPLIFT FROM:
<input type="checkbox"/> TELSTRA AUTOMATED	<input checked="" type="checkbox"/> ADMIN/2/3/4/5	<input checked="" type="checkbox"/> VIRTUAL SERVER (DEDICATED) GEN1
<input checked="" type="checkbox"/> MANUAL (SUBJECT TO SLA)	<input type="checkbox"/> NETWORKADMIN	<input checked="" type="checkbox"/> VIRTUAL SERVER (DEDICATED) GEN2
<input type="checkbox"/> CUSTOMER AUTOMATED	<input type="checkbox"/> READONLY	

OVERVIEW

A **host** is a physical server in a *Virtual Server (Dedicated) Gen2+* vDC. It will belong to a cluster of between 2 and 16 hosts, running vMotion, DRS and HA.

Before you remove a host from a cluster, you must consider the following impacts:

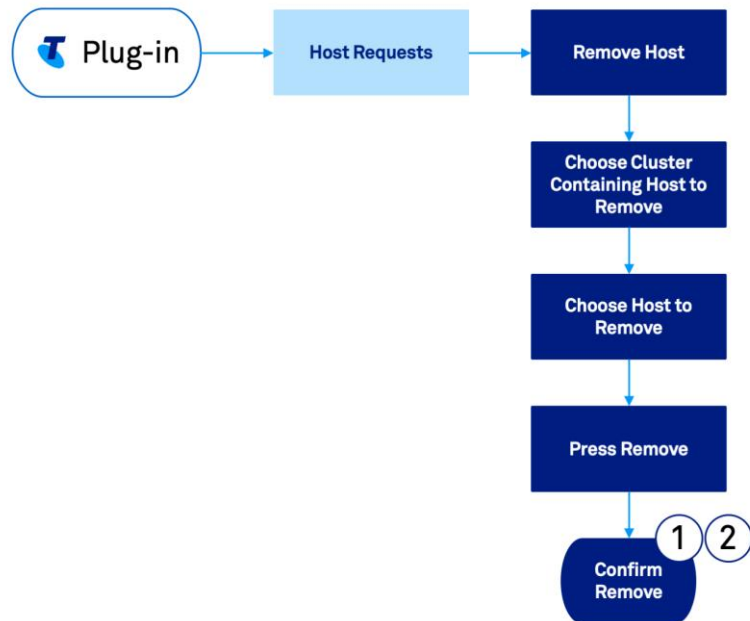
- If the host contains any active workloads when we action your request to remove it, vMotion will automatically move those workloads to other hosts in accordance with your configured DRS and HA policies. Telstra recommends that you use vMotion to appropriately manage workload migrations before you remove the host
- It is up to you to ensure that the remaining hosts in the cluster can adequately support the demands of ongoing active workloads.
- Telstra will not process a request to remove the second-last host from a cluster.

PREREQUISITES

Before you can remove a host, you must:

- a. Have moved the workloads from this host to other hosts if you do not want vMotion to do it automatically
- b. Have considered the impacts of this operation on the ability of your cluster to adequately and resiliently support remaining workloads
- c. Log into the vSphere Client for your vDC using one of your read-write administration accounts for vCenter.

PROCEDURE



NOTES

-
- 1 This is your last chance to abort the removal of the host. Once you press “Yes, Remove” you should consider this request to be irreversible
 - 2 After you submit your request, the plug-in will return a Request ID. In a future release of the plug-in, the Request ID will help you track and review your service history.
-

Chapter 12

STORAGE TASKS

TASK #ST01: ADD STORAGE

SERVICE LEVEL AGREEMENT	REQUIRED USER TYPE:	APPLIES TO UPLIFT FROM:
<input type="checkbox"/> TELSTRA AUTOMATED	<input checked="" type="checkbox"/> ADMIN/2/3/4/5	<input checked="" type="checkbox"/> VIRTUAL SERVER (DEDICATED) GEN1
<input checked="" type="checkbox"/> MANUAL (SUBJECT TO SLA)	<input checked="" type="checkbox"/> NETWORKADMIN	<input checked="" type="checkbox"/> VIRTUAL SERVER (DEDICATED) GEN2
<input type="checkbox"/> CUSTOMER AUTOMATED	<input type="checkbox"/> READONLY	

OVERVIEW

There are two main ways you can equip the hosts in a *Virtual Server (Dedicated) Gen2+* vDC with persistent storage capacity:

1. Purchase **internal storage** through *Virtual Server (Dedicated) Gen2+* and assign it to **datastores**. Datastores host the VMDKs for each VM running in *Virtual Server (Dedicated) Gen2+*
2. Acquire or provide **external storage** through some other means, which includes Telstra products such as Telstra Virtual Storage. External storage is only visible at the OS level within a VM, using protocols such as iSCSI, CIFS/SMB or NFS. It cannot host any VMDKs supported by a *Virtual Server (Dedicated) Gen2+* vDC.

This task refers specifically to the first option listed above, where you purchase internal storage and add it to a datastore. For further information on Telstra's external storage products, refer to your account team or Telstra partner.

STORAGE TIERS

Telstra offers multiple tiers of internal storage. Each tier provides storage capacity with certain performance characteristics, shown in Table 12.

TIER	STORAGE	PURPOSE
ACTIVE	Up to 1,000 IOPS per TB of purchased storage	Generally suitable for standard file, print and mixed workloads
PERFORMANCE	Up to 20,000 IOPS per TB of purchased storage	Designed to meet demanding workloads such as DBMS and analytics

TIER	STORAGE	PURPOSE
ULTRA	Exceeds 20,000 IOPS per TB of purchased storage	Suits workloads that necessitate consistently high performance such as intensive RDBMS access or virtual desktop infrastructure (VDI) environments

Table 12: Storage Tiers

Each tenancy may contain storage from one or multiple tiers. You can only buy storage from one tier per request, but you can submit multiple requests if you want to purchase storage from multiple tiers, or to buy more storage from one tier than will fit in a single datastore.

Telstra does not specifically cap the overall total amount of storage you can purchase for your vDC. However, you must assign your storage to a datastore when you purchase it, and we do apply certain limits on the capacity of individual datastores.

DATASTORES

As you purchase storage, you will assign it to a datastore. You may assign the storage to a new datastore or an existing one provided the datastore will comply with Telstra's limits:

- a. A minimum size of 250GB
- b. A maximum size of 8TB.

You can purchase storage capacity in steps of 10GB between 250GB and 1TB, and then in 1TB steps to 8TB.

A datastore consists of storage from a single tier. If you want to purchase storage from multiple tiers, you will need to purchase each tier individually and assign it to a separate new or existing datastore.

VIRTUAL MACHINES, DATASTORES AND TIERS

When you create a VM on a host in your tenancy, you will nominate one datastore as its boot volume. This is where the *Virtual Server (Dedicated) Gen2+* ESXi host will store the VMDK and associated files. It might be the only datastore the VM ever needs or uses.

If the datastore has reached 8TB in size and the VM requires more disk space, or the VM needs to use a mix of storage tiers, then you can use vSphere to add further datastores to that VM by configuring new virtual disks (vdisks). To the VM, the new virtual disks will appear as additional volumes. Each datastore will then host a VMDK that contains the respective data portion held for the associated VM.

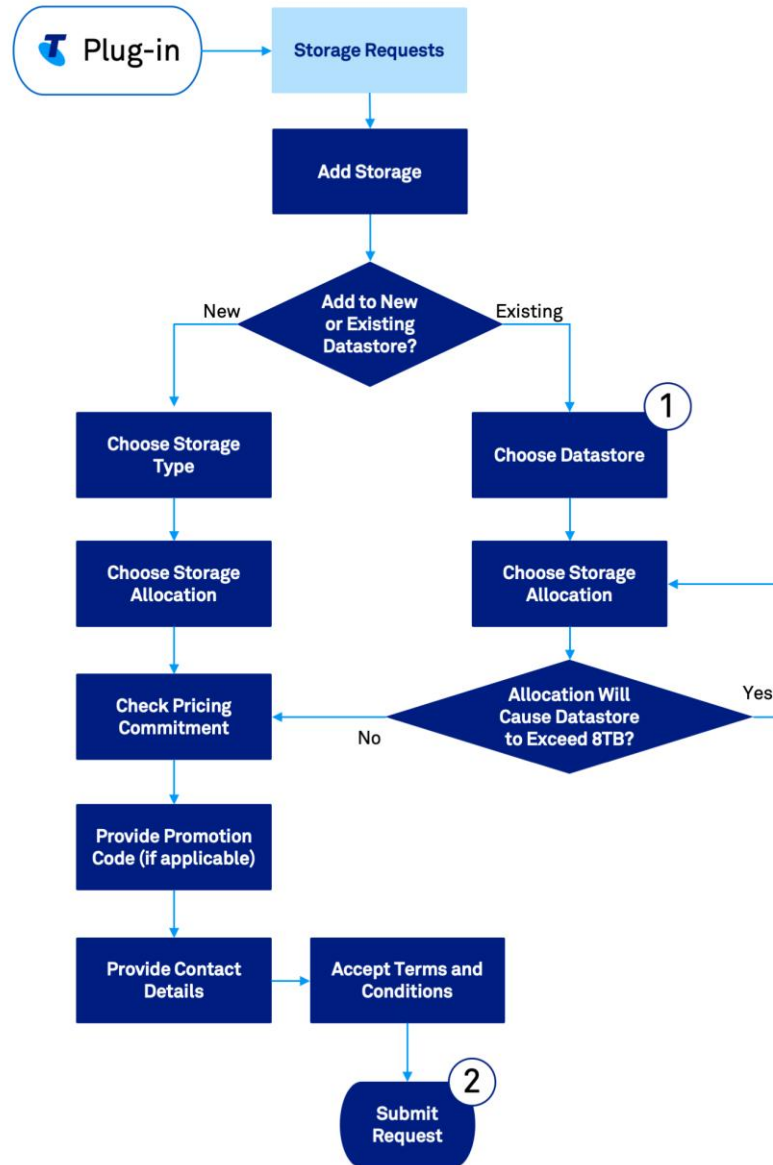
You can later move a vdisk attached to a VM between datastores using Storage vMotion. Storage vMotion can move all of the VM's vdisks or just some of them.

PREREQUISITES

Before you can add storage, you must:

- a. Log into the vSphere Client for your vDC using one of your read-write administration accounts for vCenter.

PROCEDURE



NOTES

1 The plug-in does not show the storage type for the datastore you choose in this step. It is up to you to verify that the datastore already contains the correct storage type for your needs. To specify another storage type, you will need to select a different existing datastore or add a new datastore

2 After you submit your request, the plug-in will return a Request ID. In a future release of the plug-in, the Request ID will help you track and review your service history.

TASK #ST02: REMOVE STORAGE

SERVICE LEVEL AGREEMENT	REQUIRED USER TYPE:	APPLIES TO UPLIFT FROM:
<input type="checkbox"/> TELSTRA AUTOMATED	<input checked="" type="checkbox"/> ADMIN/2/3/4/5	<input checked="" type="checkbox"/> VIRTUAL SERVER (DEDICATED) GEN1
<input checked="" type="checkbox"/> MANUAL (SUBJECT TO SLA)	<input checked="" type="checkbox"/> NETWORKADMIN	<input checked="" type="checkbox"/> VIRTUAL SERVER (DEDICATED) GEN2
<input type="checkbox"/> CUSTOMER AUTOMATED	<input type="checkbox"/> READONLY	

OVERVIEW

Virtual Server (Dedicated) Gen2+ allows you to remove storage you no longer require. 'Remove storage' means remove an entire datastore in one operation. You cannot downsize or partly remove a datastore. All data contained in the datastore is destroyed and irrecoverable after Telstra acts on this request.

Telstra cannot remove a datastore if it contains:

- VMDKs for any VMs, whether they are active or stopped
- VM templates.

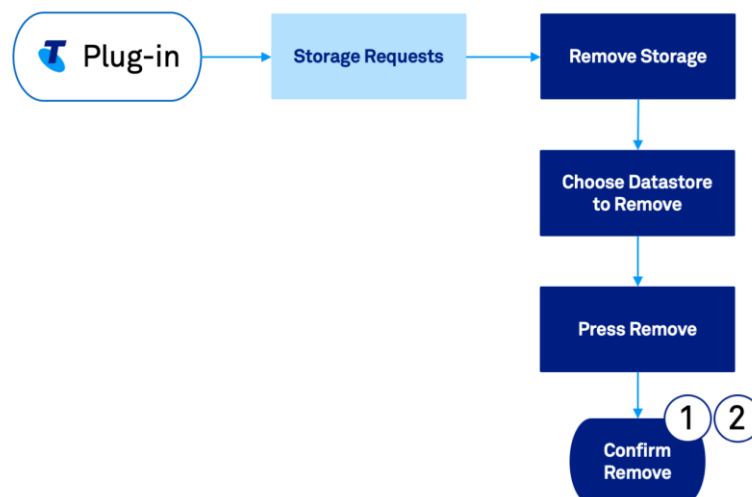
You must ensure you de-associate the datastore from any registered VMs (or delete the VMs) and remove any VM templates it contains before you submit this request.

PREREQUISITES

Before you can remove storage:

- a. We recommend you back up the data contained in the datastore you will remove
- b. You must have removed all VMDKs and VM templates from, the datastore
- c. You will need to log into the vSphere Client for your vDC using one of your read-write administration accounts for vCenter.

PROCEDURE



NOTES

- ① This is your last chance to abort the removal of the host. Once you press “Yes, Remove” you should consider this request to be irreversible
 - ② After you submit your request, the plug-in will return a Request ID. In a future release of the plug-in, the Request ID will help you track and review your service history.
-

Chapter 13

PUBLIC ADDRESSING TASKS

TASK #PA01: ADD A PUBLIC IP ADDRESS (RANGE)

SERVICE LEVEL AGREEMENT	REQUIRED USER TYPE:	APPLIES TO UPLIFT FROM:
<input type="checkbox"/> TELSTRA AUTOMATED	<input checked="" type="checkbox"/> ADMIN/2/3/4/5	<input checked="" type="checkbox"/> VIRTUAL SERVER (DEDICATED) GEN1
<input checked="" type="checkbox"/> MANUAL (SUBJECT TO SLA)	<input checked="" type="checkbox"/> NETWORKADMIN	<input checked="" type="checkbox"/> VIRTUAL SERVER (DEDICATED) GEN2
<input type="checkbox"/> CUSTOMER AUTOMATED	<input type="checkbox"/> READONLY	

OVERVIEW

You will need to request public IP addresses from Telstra if you plan to implement a public network topology in *Virtual Server (Dedicated) Gen2+* and want to reach your hosts from the Internet via your Dedicated Public ESG without resorting to NAT via the single usable public IP address we configured during uplift. *Virtual Server (Dedicated) Gen2+* does not support BYO public address ranges, nor Telstra-supplied ranges obtained from other products such as TID or MIG.

Furthermore, if you have multiple vDCs, your vSphere client must be logged into the correct vDC at the time you submit your request. You cannot order a public IP address range for vDC A from a vSphere client logged into vDC B. Neither can you arbitrarily move ranges from one vDC to another, even within the same physical DC, because Telstra uses external networking configurations that associate the range with the vDC to which it was assigned.

You can request ranges in any size between /26 and /32, inclusive. Telstra's fees vary according to the size of the range.

When fulfilling your request, Telstra supplies a 'floating' range. That means that you are free to use the range within the *Virtual Server (Dedicated) Gen2+* vDC to suit your desired public topology. You can also further segment the range if you wish.

ROUTING

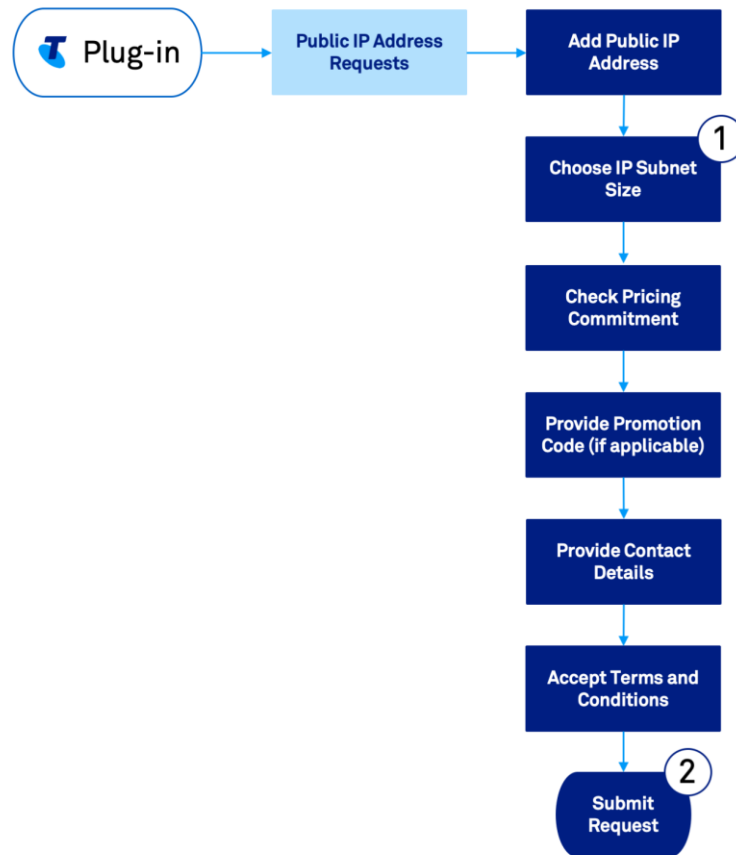
Telstra will populate the Shared Public Routers with a static route to the public IP address range that points to your Dedicated Public ESG as the next hop. It is up to you to configure your Dedicated Public ESG with the correct routes to reach the range inside your vDC.

PREREQUISITES

Before you can add a public IP address, you must:

- a. Log into the vSphere Client for your vDC using one of your read-write administration accounts for vCenter.

PROCEDURE



NOTES

-
- ① The plug-in will show you the equivalent number of usable hosts in a subnet of each size. This is based on the presumption that the subnet will be used in a single block, with one address consumed on the default gateway for the segment hosting the block
-
- ② After you submit your request by pressing “Add Public IP Address”, the plug-in will return a Request ID. In a future release of the plug-in, the Request ID will help you track and review your service history.
-

TASK #PA02: REMOVE A PUBLIC IP ADDRESS

SERVICE LEVEL AGREEMENT

- TELSTRA AUTOMATED
- MANUAL (SUBJECT TO SLA)
- CUSTOMER AUTOMATED

REQUIRED USER TYPE:

- ADMIN/2/3/4/5
- NETWORKADMIN
- READONLY

APPLIES TO UPLIFT FROM:

- VIRTUAL SERVER (DEDICATED) GEN1
- VIRTUAL SERVER (DEDICATED) GEN2

OVERVIEW

You can release a *Virtual Server (Dedicated) Gen2+* public IP address range back to Telstra if you no longer need it.

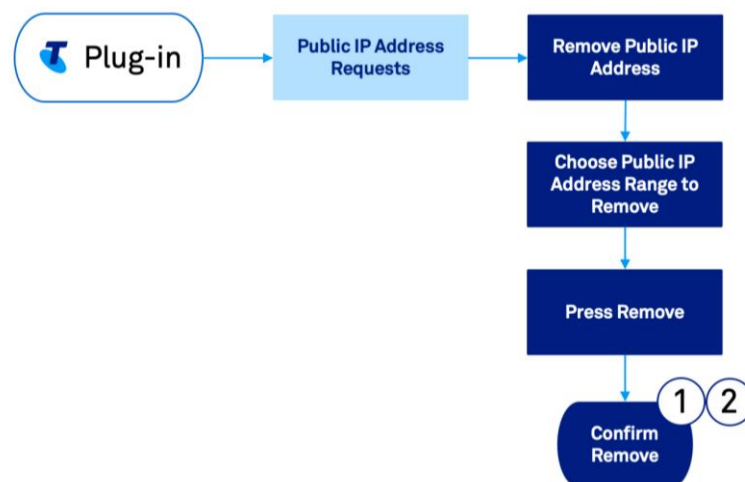
You must be certain that you wish to complete this action before submitting your request. After you submit your request and we act on it, you should consider it irreversible. We may not be able to re-assign the range back to you if you change your mind or have made a mistake.

PREREQUISITES

Before you can remove a Public IP address range:

- a. We recommend you remove all affected addresses from any resources in your vDC that may still have them configured
- b. You will need to log into the vSphere Client for your vDC using one of your read-write administration accounts for vCenter.

PROCEDURE



NOTES

- 1 This is your last chance to abort the removal of the host. Once you press "Yes, Remove" you should consider this request to be irreversible
-

2

After you submit your request, the plug-in will return a Request ID. In a future release of the plug-in, the Request ID will help you track and review your service history.

Chapter 14

SERVICE REQUEST TASKS

TASK #SR01: CONFIGURE BACKUP

SERVICE LEVEL AGREEMENT	REQUIRED USER TYPE:	APPLIES TO UPLIFT FROM:
<input type="checkbox"/> TELSTRA AUTOMATED	<input checked="" type="checkbox"/> ADMIN/2/3/4/5	<input checked="" type="checkbox"/> VIRTUAL SERVER (DEDICATED) GEN1
<input checked="" type="checkbox"/> MANUAL (SUBJECT TO SLA)	<input checked="" type="checkbox"/> NETWORKADMIN	<input checked="" type="checkbox"/> VIRTUAL SERVER (DEDICATED) GEN2
<input type="checkbox"/> CUSTOMER AUTOMATED	<input type="checkbox"/> READONLY	

OVERVIEW

This service request is applicable to customers who use Telstra Managed Backup (TMB) with Virtual Server (Dedicated) Gen2+.

Telstra Operations constructs scheduled backup jobs for TMB. The TMB agent(s) in your vDC will contact the TMB server to retrieve the backup schedule and the tasks to complete.

You use this service request to schedule a new regular VM backup event or to run an ad hoc backup job.

Telstra Operations may contact you submission to ask for further information or clarify your request.

CONSIDERATIONS FOR VM BACKUPS

You can back up your VMs according to daily schedules or run an ad hoc backup job due to special circumstances. An ad hoc backup may supplement regular scheduled backups for the VM or be a one-off job.

The default action for a TMB Virtual Server backup is to store a copy of everything (that has changed) in the file system on the boot volume. Since you might have mounted additional disks in the VM that you wish to backup as well, you can nominate those in the same request.

Backup size helps to determine the price we charge you to back up your data. Therefore, you might not want to back up the OS itself or your application executables but focus instead on data files. If this is the case, you can specify drives, folders and files to exclude from the backup event.

Telstra Managed Backup uses the Dell EMC Avamar backup system. Avamar agents are compatible with many common operating systems, but there will be times where a new OS or version is awaiting support.

Dell EMC provides a public compatibility portal that you can use to validate support for your applications and operating systems. You will find the portal at:

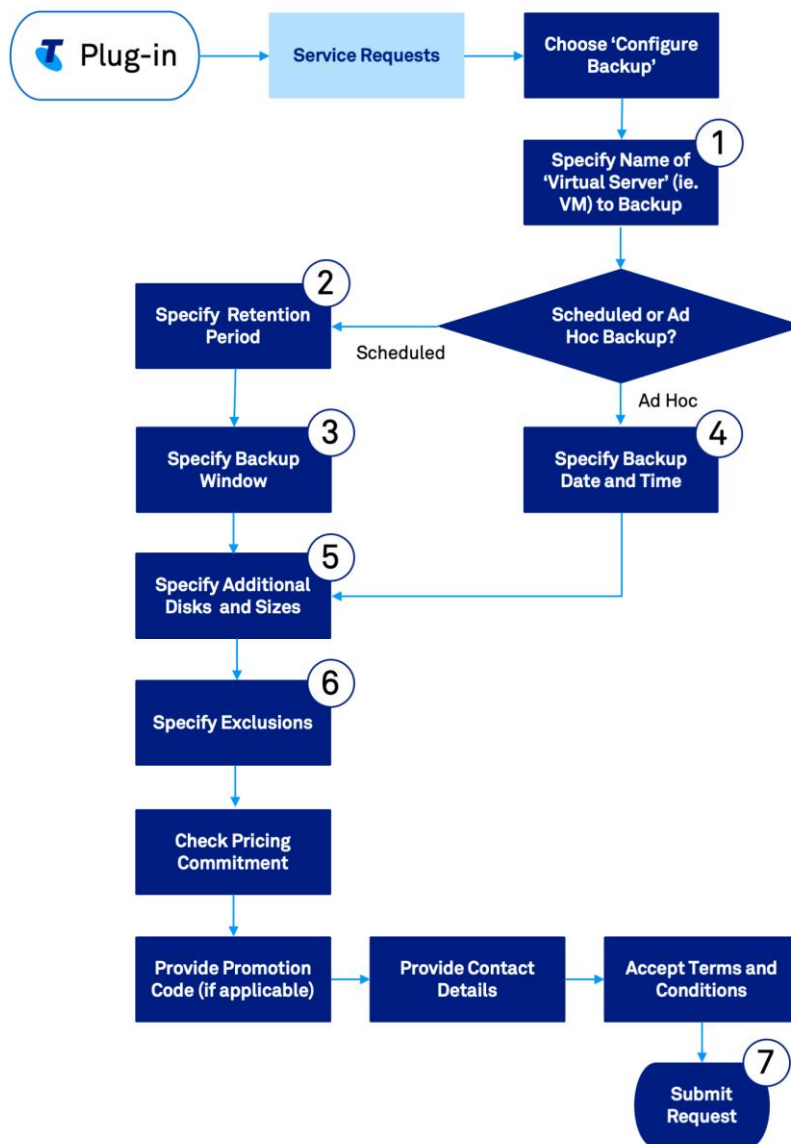
<http://compatibilityguide.emc.com:8080/CompGuideApp/>

PREREQUISITES

Before you can add an application to a backup:

- a. You must be an existing customer of TMB
- b. You should validate your OS compatibility using Dell EMC's online portal
- c. You will need to log into the vSphere client for your vDC using any of your read-write administration accounts.

PROCEDURE



NOTES

- 1 Check OS and application compatibility with Dell EMC Avamar

- ② You specify a retention period of 1 week, 1 month, 1 quarter, 1 year or 7 years. TMB consolidates your daily backups to monthly backups after 3 months

- ③ The backup window you choose is advisory only. Telstra reserves the right to negotiate this window with you when overall demand may cause your backup to exceed the times you nominated

- ④ We schedule the backup to begin at your designated time

- ⑤ The disk size will help us estimate the demand on our backup storage resources. The actual amount of backup data we store for you affects the price we charge

- ⑥ The default behaviour for the backup event is to backup all available objects on the VM or disk

- ⑦ After you submit your request, the plug-in will return a Request ID. In a future release of the plug-in, the Request ID will help you track and review your service history.

TASK #SR02: MODIFY BACKUP

SERVICE LEVEL AGREEMENT	REQUIRED USER TYPE:	APPLIES TO UPLIFT FROM:
<input type="checkbox"/> TELSTRA AUTOMATED	<input checked="" type="checkbox"/> ADMIN/2/3/4/5	<input checked="" type="checkbox"/> VIRTUAL SERVER (DEDICATED) GEN1
<input checked="" type="checkbox"/> MANUAL (SUBJECT TO SLA)	<input checked="" type="checkbox"/> NETWORKADMIN	<input checked="" type="checkbox"/> VIRTUAL SERVER (DEDICATED) GEN2
<input type="checkbox"/> CUSTOMER AUTOMATED	<input type="checkbox"/> READONLY	

OVERVIEW

This service request is applicable to customers who use Telstra Managed Backup (TMB) with Virtual Server (Dedicated) Gen2+.

Telstra Operations constructs scheduled backup jobs for TMB. The TMB agent(s) in your vDC will contact the TMB server to retrieve the backup schedule and the tasks to complete.

You use this service request to modify or stop a regular VM backup event.

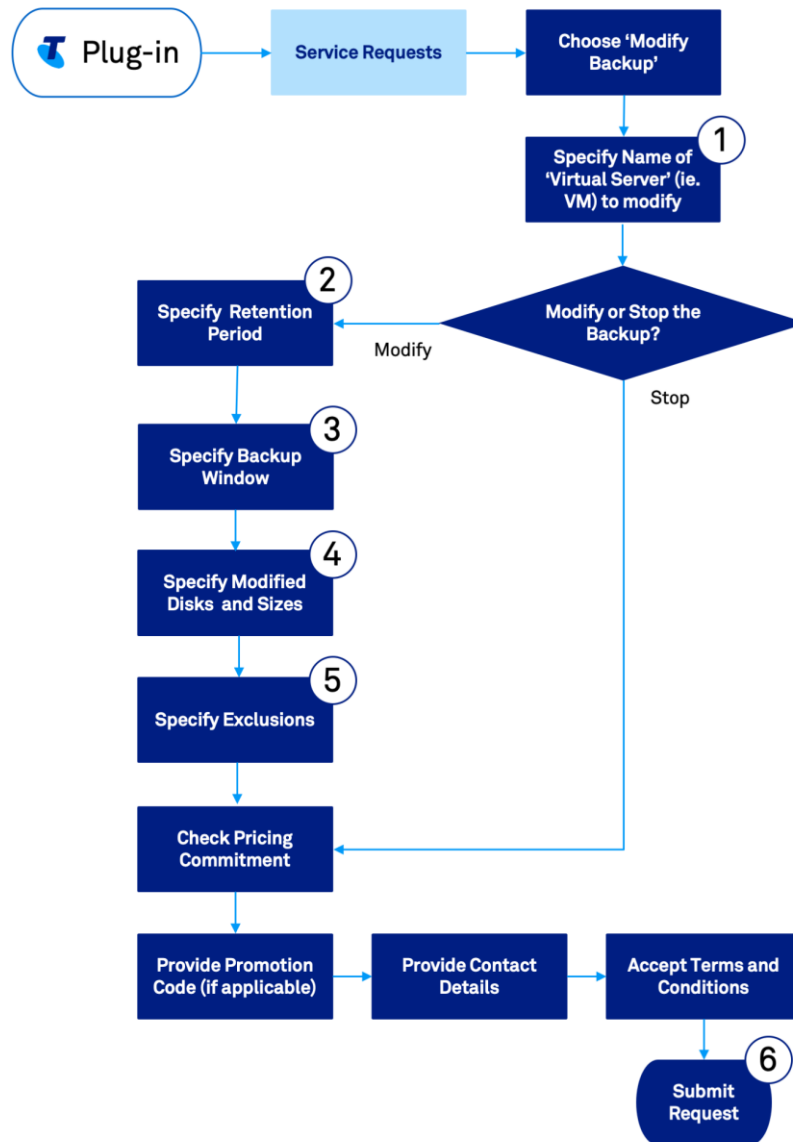
Telstra Operations may contact you submission to ask for further information or clarify your request.

PREREQUISITES

Before you can add an application to a backup:

- a. You must be an existing customer of TMB
- b. You must have an existing scheduled backup event for the VM (virtual server) nominated in your service request
- c. You will need to log into the vSphere client for your vDC using any of your read-write administration accounts.

PROCEDURE



NOTES

- 1 This service request only modifies existing backup schedules. Use “Configure Backup” to specify a backup schedule for a new VM
- 2 You specify a retention period of 1 week, 1 month, 1 quarter, 1 year or 7 years. TMB consolidates your daily backups to monthly backups after 3 months
- 3 The backup window you choose is advisory only. Telstra reserves the right to negotiate this window with you when overall demand may cause your backup to exceed the times you nominated
- 4 The disk size will help us estimate the demand on our backup storage resources. The actual amount of backup data we store for you affects the price we charge

5 The default behaviour for the backup event is to backup all available objects on the VM or disk

6 After you submit your request, the plug-in will return a Request ID. In a future release of the plug-in, the Request ID will help you track and review your service history.

TASK #SR03: ADD APPLICATION TO BACKUP

SERVICE LEVEL AGREEMENT	REQUIRED USER TYPE:	APPLIES TO UPLIFT FROM:
<input type="checkbox"/> TELSTRA AUTOMATED	<input checked="" type="checkbox"/> ADMIN/2/3/4/5	<input checked="" type="checkbox"/> VIRTUAL SERVER (DEDICATED) GEN1
<input checked="" type="checkbox"/> MANUAL (SUBJECT TO SLA)	<input checked="" type="checkbox"/> NETWORKADMIN	<input checked="" type="checkbox"/> VIRTUAL SERVER (DEDICATED) GEN2
<input type="checkbox"/> CUSTOMER AUTOMATED	<input type="checkbox"/> READONLY	

OVERVIEW

This service request is applicable to customers who use Telstra Managed Backup (TMB) with Virtual Server (Dedicated) Gen2+.

Telstra Operations constructs scheduled backup jobs for TMB. The TMB agent(s) in your vDC will contact the TMB server to retrieve the backup schedule and the tasks to complete.

You use this service request to include a new application during the execution of your backup jobs.

Telstra Operations may contact you submission to ask for further information or clarify your request.

CONSIDERATIONS FOR APPLICATION BACKUPS

Backing up certain applications such as database management systems is often more complex than simply copying files or directories. Rather, backup systems may need to use privileged agents that can 'converse' with these applications to stop or pause processing during the backup event, as well as to capture application-specific parameters and configuration settings that aid recovery after a failure.

The agents are typically customised for each application, and in some cases for different versions of the same application.

Telstra Managed Backup uses the Dell EMC Avamar backup system. Avamar agents are compatible with many common applications, but there will be times where a new application is awaiting support.

Dell EMC provides a public compatibility portal that you can use to validate support for your application and operating systems. You will find the portal at:

<http://compatibilityguide.emc.com:8080/CompGuideApp/>

PREREQUISITES

Before you can add an application to a backup:

- a. You must be an existing customer of TMB
- b. You should validate your application compatibility using Dell EMC's online portal
- c. You will need to log into the vSphere client for your vDC using any of your read-write administration accounts.

PROCEDURE



NOTES

-
- ① Check application compatibility with Dell EMC Avamar

 - ② The application version is important. Agent support might not yet be available for newer versions

 - ③ For some applications, the data file path is not required

 - ④ The application size will help us estimate the demand on our backup storage resources. The actual amount of backup data we store for you affects the price we charge

5

After you submit your request, the plug-in will return a Request ID. In a future release of the plug-in, the Request ID will help you track and review your service history.

TASK #SR04: ADD DISK TO BACKUP

SERVICE LEVEL AGREEMENT	REQUIRED USER TYPE:	APPLIES TO UPLIFT FROM:
<input type="checkbox"/> TELSTRA AUTOMATED	<input checked="" type="checkbox"/> ADMIN/2/3/4/5	<input checked="" type="checkbox"/> VIRTUAL SERVER (DEDICATED) GEN1
<input checked="" type="checkbox"/> MANUAL (SUBJECT TO SLA)	<input checked="" type="checkbox"/> NETWORKADMIN	<input checked="" type="checkbox"/> VIRTUAL SERVER (DEDICATED) GEN2
<input type="checkbox"/> CUSTOMER AUTOMATED	<input type="checkbox"/> READONLY	

OVERVIEW

This service request is applicable to customers who use Telstra Managed Backup (TMB) with Virtual Server (Dedicated) Gen2+.

Telstra Operations constructs scheduled backup jobs for TMB. The TMB agent(s) in your vDC will contact the TMB server to retrieve the backup schedule and the tasks to complete.

You use this service request to include a new disk during the execution of your backup jobs.

Telstra Operations may contact you submission to ask for further information or clarify your request.

CONSIDERATIONS FOR DISK BACKUPS

When you add a disk to a configured backup job, you will generally identify it using:

- Its drive letter, on a Windows server
- Its mount point, on a Linux server.

Hence, you will need to provide us the server name along with the disk identifier.

While Dell EMC Avamar does have the ability to directly backup certain compatible NAS drives, this is not available with TMB. If you wish to back up a NAS drive (NFS, CIFS/SMB or iSCSI) you will need to do it through the OS-executed agent on a server (ie. VM).

PREREQUISITES

Before you can add a disk to a backup:

- a. You must be an existing customer of TMB
- b. The server attaching the disk must be already scheduled for backups in TMB. (If you need to add the server along with the disk, use service request Task #SR01: Configure Backup)
- c. You will need to log into the vSphere client for your vDC using an administration account.

PROCEDURE



NOTES

- 1 The ID will generally consist of a virtual server (ie. VM) name and drive letter (Windows) or mount point (Linux). You cannot nominate a NAS except through a server designator
- 2 The disk size will help us estimate the execution time for the backup and the consumption of storage resources. The actual size also affects the price we charge you for storing your backup data
- 3 The default behaviour for the backup event is to attempt to backup all available objects on the disk
- 4 The disk size will help us estimate the demand on our backup storage resources. The actual amount of backup data we store for you affects the price we charge
- 5 After you submit your request, the plug-in will return a Request ID. In a future release of the plug-in, the Request ID will help you track and review your service history.

TASK #SR05: RESTORE FROM BACKUP

SERVICE LEVEL AGREEMENT	REQUIRED USER TYPE:	APPLIES TO UPLIFT FROM:
<input type="checkbox"/> TELSTRA AUTOMATED	<input checked="" type="checkbox"/> ADMIN/2/3/4/5	<input checked="" type="checkbox"/> VIRTUAL SERVER (DEDICATED) GEN1
<input checked="" type="checkbox"/> MANUAL (SUBJECT TO SLA)	<input checked="" type="checkbox"/> NETWORKADMIN	<input checked="" type="checkbox"/> VIRTUAL SERVER (DEDICATED) GEN2
<input type="checkbox"/> CUSTOMER AUTOMATED	<input type="checkbox"/> READONLY	

OVERVIEW

This service request is applicable to customers who use Telstra Managed Backup (TMB) with Virtual Server (Dedicated) Gen2+.

You can generally restore files from TMB backups yourself using the Avamar console. This is the fastest option available to you. However, if you need assistance because of the type of restoration you need to perform or have a related professional services contract with us and would rather Telstra complete the task, then you can submit this service request.

Telstra Operations may contact you submission to ask for further information or clarify your request.

CONSIDERATIONS FOR RESTORATION OPERATIONS

You can use the Avamar console utility to initiate file-by-file restoration. After you choose the applicable version of the file(s) from the library of available backups, Avamar automatically completes the restoration operation.

While the generic Avamar system includes a capability to perform a full system restoration, Telstra Managed Backup does not support full system restoration as a standard function, and it is not offered in the Avamar console.

You can use this service request to seek help from to rebuild a VM. Our Operations staff will collaborate with you to help you:

- Recover the basic OS into a new VM
- Restore the virtual system state (VSS) of the VM
- Commence file system restoration after the basic server is running.

PREREQUISITES

Before you can add an application to a backup:

- a. You must be an existing customer of TMB
- b. You will need to log into the vSphere client for your vDC using an administration account.

PROCEDURE



NOTES

- ① For restoration from recent backups, we only need the actual date of the backup. After three months, we consolidate your data into monthly backups. For these, we need a start and end date to identify the correct consolidated backup
- ② The types of files may affect the way the restoration proceeds. For example, it might require the Avamar agent to login to an application
- ③ You can choose to restore to the original location from which the data was backed up, or nominate an alternative location

4

After you submit your request, the plug-in will return a Request ID. In a future release of the plug-in, the Request ID will help you track and review your service history.

TASK #SR06: MANAGE BACKUP ACCOUNTS

SERVICE LEVEL AGREEMENT	REQUIRED USER TYPE:	APPLIES TO UPLIFT FROM:
<input type="checkbox"/> TELSTRA AUTOMATED	<input checked="" type="checkbox"/> ADMIN/2/3/4/5	<input checked="" type="checkbox"/> VIRTUAL SERVER (DEDICATED) GEN1
<input checked="" type="checkbox"/> MANUAL (SUBJECT TO SLA)	<input checked="" type="checkbox"/> NETWORKADMIN	<input checked="" type="checkbox"/> VIRTUAL SERVER (DEDICATED) GEN2
<input type="checkbox"/> CUSTOMER AUTOMATED	<input type="checkbox"/> READONLY	

OVERVIEW

This service request is applicable to customers who use Telstra Managed Backup (TMB) with Virtual Server (Dedicated) Gen2+.

You can perform some tasks in TMB unassisted using the Avamar console. The console requires a username and password. You can have multiple accounts, each with its own set of permissions.

Occasionally you will need to add an Avamar user, change the password for it, or change some other permissions. You can do so using this service request.

Telstra Operations may contact you submission to ask for further information or clarify your request.

CONSIDERATIONS FOR BACKUP ACCOUNT IDENTIFICATION

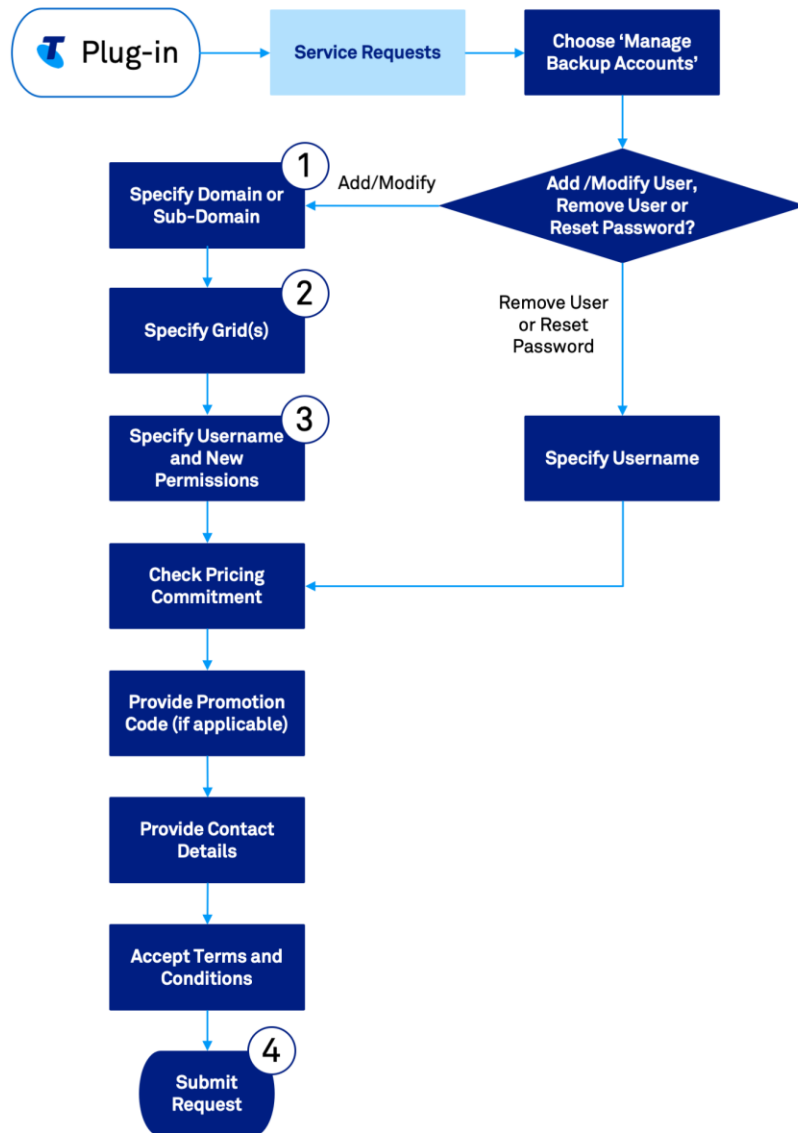
When you request a change to a TMB user account, you will need to provide your TMB Domain/Sub-domain ID and Grid ID. You use these parameters to log into your Avamar client. Alternatively, Telstra will have supplied them to you in an email when we commissioned your TMB service.

PREREQUISITES

Before you can add an application to a backup:

- a. You must be an existing customer of TMB
- b. You will need to log into the vSphere client for your vDC using an administration account.

PROCEDURE



NOTES

-
- 1 This is the domain/sub-domain ID you use to log into your Avamar client
-
- 2 This is the Grid ID you use to log into your Avamar client
-
- 3 Examples of permissions are:
- Backup only
 - Restore only
 - Backup and restore
-
- 4 After you submit your request, the plug-in will return a Request ID. In a future release of the plug-in, the Request ID will help you track and review your service history.
-

TASK #SR07: MODIFY IPSEC

SERVICE LEVEL AGREEMENT	REQUIRED USER TYPE:	APPLIES TO UPLIFT FROM:
<input type="checkbox"/> TELSTRA AUTOMATED	<input checked="" type="checkbox"/> ADMIN/2/3/4/5	<input checked="" type="checkbox"/> VIRTUAL SERVER (DEDICATED) GEN1
<input checked="" type="checkbox"/> MANUAL (SUBJECT TO SLA)	<input checked="" type="checkbox"/> NETWORKADMIN	<input checked="" type="checkbox"/> VIRTUAL SERVER (DEDICATED) GEN2
<input type="checkbox"/> CUSTOMER AUTOMATED	<input type="checkbox"/> READONLY	

OVERVIEW

If you have used IPsec access to your vDC in the past, your legacy IPsec concentrator will still be running after we uplift your vDC to Virtual Server (Dedicated) Gen2+.

You can use this service request to request us to change the Peer IP address for the IPsec configuration in the legacy IP concentrator. We consider any other modifications to your settings, such as Phase 1 or Phase 2 parameters, to be a complex change requiring migration off the legacy IPsec concentrator and onto a new concentrator you configure in your Dedicated Public ESG.

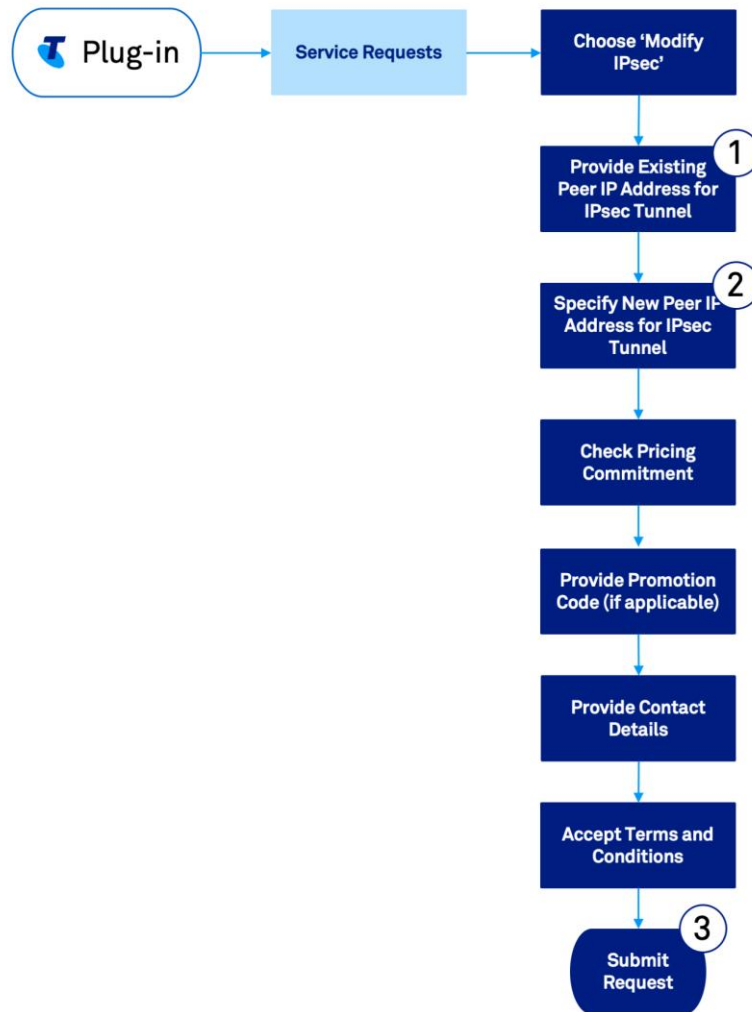
Telstra Operations may contact you submission to ask for further information or clarify your request.

PREREQUISITES

Before you can modify your IPsec configuration:

- a. You will need to know the new Peer IP address of the IPsec concentrator at your site
- b. You will need to log into the vSphere client for your vDC using an administration account.

PROCEDURE



NOTES

-
- ① This is the existing Peer IP address. It will be a static IP address unique to your site
-
- ② This is the new Peer IP address. It must be a static IP address unique to your site
-
- ③ After you submit your request, the plug-in will return a Request ID. In a future release of the plug-in, the Request ID will help you track and review your service history.
-

TASK #SR08: DELETE IPSEC

SERVICE LEVEL AGREEMENT	REQUIRED USER TYPE:	APPLIES TO UPLIFT FROM:
<input type="checkbox"/> TELSTRA AUTOMATED	<input checked="" type="checkbox"/> ADMIN/2/3/4/5	<input checked="" type="checkbox"/> VIRTUAL SERVER (DEDICATED) GEN1
<input checked="" type="checkbox"/> MANUAL (SUBJECT TO SLA)	<input checked="" type="checkbox"/> NETWORKADMIN	<input checked="" type="checkbox"/> VIRTUAL SERVER (DEDICATED) GEN2
<input type="checkbox"/> CUSTOMER AUTOMATED	<input type="checkbox"/> READONLY	

OVERVIEW

If you have used IPsec access to your vDC in the past, your legacy IPsec concentrator will still be running after we uplift your vDC to Virtual Server (Dedicated) Gen2+.

You can use this service request can request us to remove the IPsec configuration for a site. After we remove the configuration, your site will need to contact Virtual Server (Dedicated) Gen2+ by other means, which might be through a new IPsec concentrator you have configured in your Dedicated Public ESG.

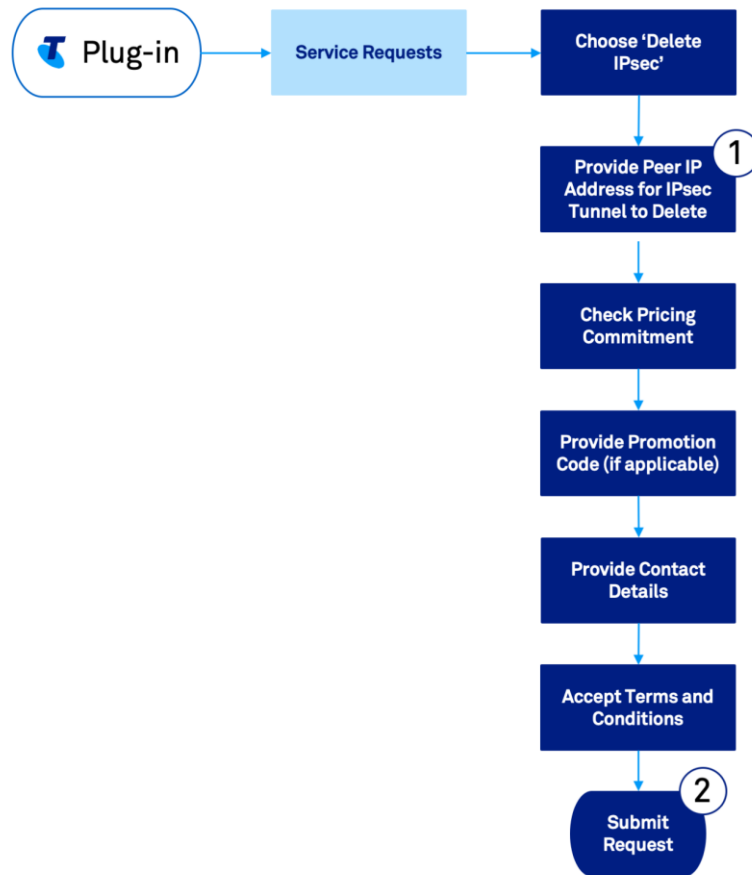
Telstra Operations may contact you submission to ask for further information or clarify your request.

PREREQUISITES

Before you can delete your IPsec configuration:

- a. You will need to know the Peer IP address of the IPsec concentrator you wish to remove
- b. You will need to log into the vSphere client for your vDC using an administration account.

PROCEDURE



NOTES

-
- 1 This is the existing Peer IP address. It will be a static IP address unique to your site
-
- 2 After you submit your request, the plug-in will return a Request ID. In a future release of the plug-in, the Request ID will help you track and review your service history.
-

TASK #SR09: REQUEST CURRENT LOAD BALANCER CONFIGURATION

SERVICE LEVEL AGREEMENT	REQUIRED USER TYPE:	APPLIES TO UPLIFT FROM:
<input type="checkbox"/> TELSTRA AUTOMATED	<input checked="" type="checkbox"/> ADMIN/2/3/4/5	<input checked="" type="checkbox"/> VIRTUAL SERVER (DEDICATED) GEN1
<input checked="" type="checkbox"/> MANUAL (SUBJECT TO SLA)	<input checked="" type="checkbox"/> NETWORKADMIN	<input type="checkbox"/> VIRTUAL SERVER (DEDICATED) GEN2
<input type="checkbox"/> CUSTOMER AUTOMATED	<input type="checkbox"/> READONLY	

OVERVIEW

If you used a public or private load balancer in the past and we uplifted your vDC from Virtual Server (Dedicated) Generation 1, your old load balancer will still be running with its original configuration. You cannot directly see or control a legacy load balancer.

If you submit this service request, we will send you a copy of the configuration for your public or private load balancer operating at the virtual IP address and protocol port number you provide.

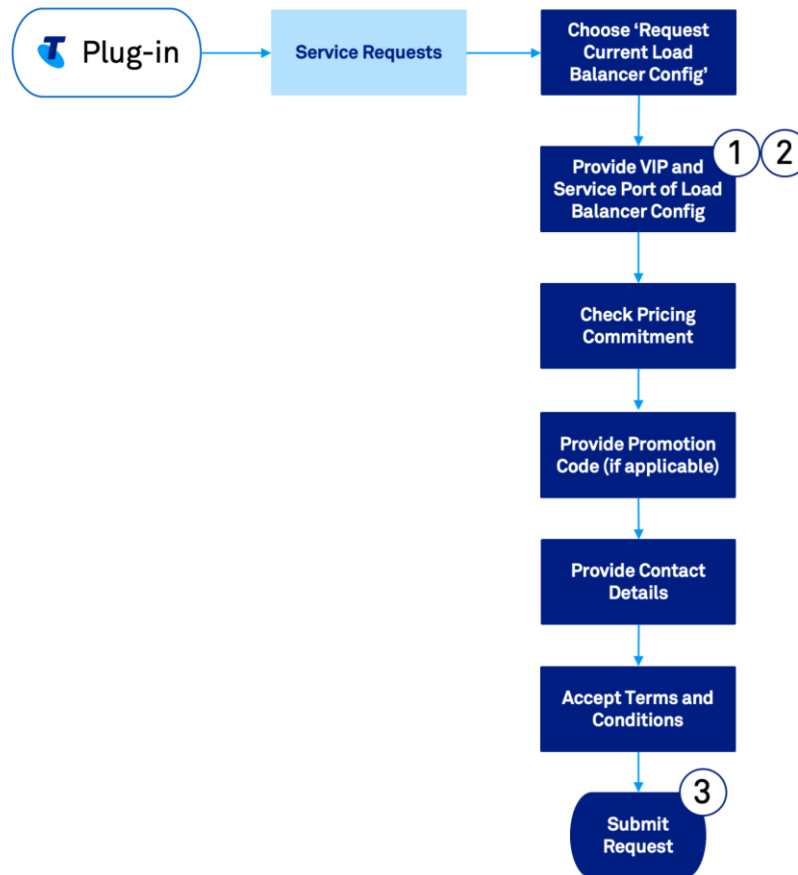
Telstra Operations may contact you submission to ask for further information or clarify your request.

PREREQUISITES

Before you can request your current load balancer configuration:

- a. You must (still) use a legacy public or private load balancer originally provided under Virtual Server (Dedicated) Gen1
- b. You will need to know the virtual IP address and protocol port number of the load balancer for which you want a copy of the configuration
- c. You will need to log into the vSphere client for your vDC using an administration account.

PROCEDURE



NOTES

-
- 1 The virtual IP address (VIP) is the destination IP address clients use to contact the application. It may not be the source IP address the load balancer uses to forward transactions to the application server(s) in the pool
 - 2 The service port is the destination protocol port number clients use to contact the application. It may not be the source port the load balancer uses to forward transactions to the application server(s) in the pool
 - 3 After you submit your request, the plug-in will return a Request ID. In a future release of the plug-in, the Request ID will help you track and review your service history.
-

TASK #SR10: MODIFY LOAD BALANCER

SERVICE LEVEL AGREEMENT	REQUIRED USER TYPE:	APPLIES TO UPLIFT FROM:
<input type="checkbox"/> TELSTRA AUTOMATED	<input checked="" type="checkbox"/> ADMIN/2/3/4/5	<input checked="" type="checkbox"/> VIRTUAL SERVER (DEDICATED) GEN1
<input checked="" type="checkbox"/> MANUAL (SUBJECT TO SLA)	<input checked="" type="checkbox"/> NETWORKADMIN	<input type="checkbox"/> VIRTUAL SERVER (DEDICATED) GEN2
<input type="checkbox"/> CUSTOMER AUTOMATED	<input type="checkbox"/> READONLY	

OVERVIEW

If you used a public or private load balancer in the past and we uplifted your vDC from Virtual Server (Dedicated) Generation 1, your old load balancer will still be running with its original configuration. You cannot directly see or control a legacy load balancer.

Virtual Server (Dedicated) Generation 1 used Cisco ACE-based load balancers. Telstra encourages you to replace them with another you can configure, control and manage yourself in a VMware NSX ESG.

If you choose to continue with your legacy load balancer, you can ask us to make basic configuration changes by submitting this request and providing its virtual IP address and protocol port number.

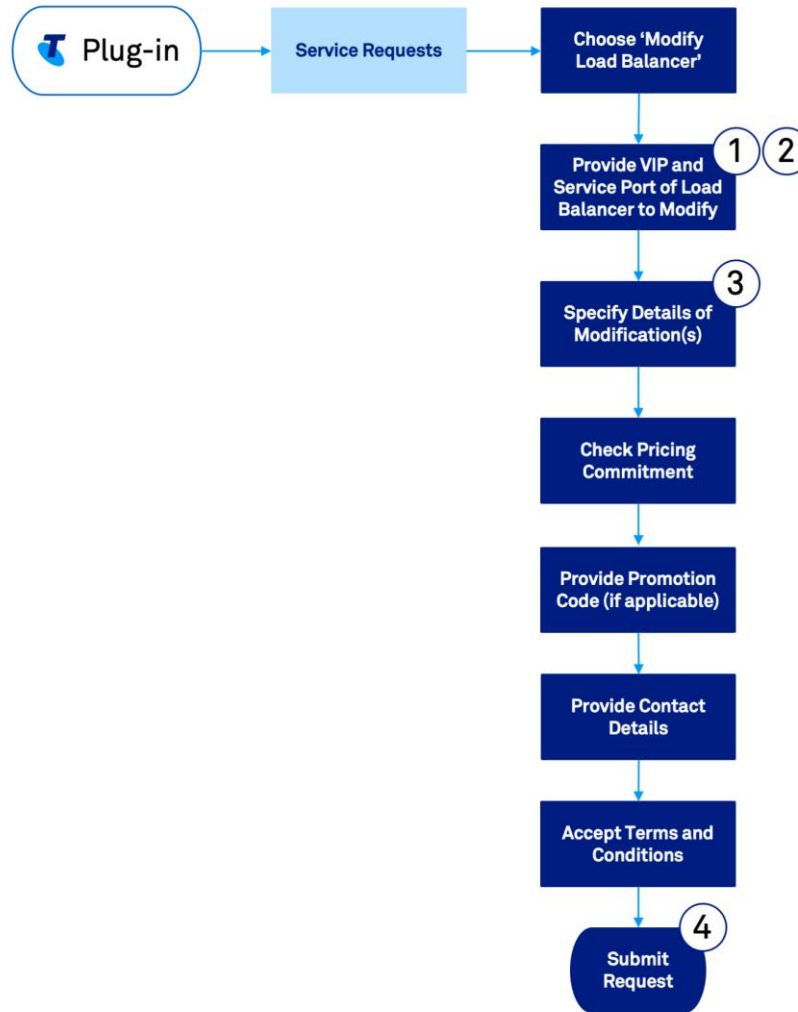
Telstra Operations may contact your submission to ask for further information or clarify your request.

PREREQUISITES

Before you can modify your load balancer configuration:

- a. You must (still) use a legacy public or private load balancer originally provided under Virtual Server (Dedicated) Gen1
- b. You will need to know the virtual IP address and protocol port number of the load balancer for which you want us to modify the configuration
- c. You will need to log into the vSphere client for your vDC using an administration account.

PROCEDURE



NOTES

- ① The virtual IP address (VIP) is the destination IP address clients use to contact the application. It may not be the source IP address the load balancer uses to forward transactions to the application server(s) in the pool
- ② The service port is the destination protocol port number clients use to contact the application. It may not be the source port the load balancer uses to forward transactions to the application server(s) in the pool
- ③ Details of the modifications you require may include:
 - The address(es) of the target server(s) and/or protocol port number on which they respond
 - Load balancing method
 - Association persistence
 - Health check method
- ④ After you submit your request, the plug-in will return a Request ID. In a future release of the plug-in, the Request ID will help you track and review your service history.

TASK #SR11: REMOVE LOAD BALANCER

SERVICE LEVEL AGREEMENT	REQUIRED USER TYPE:	APPLIES TO UPLIFT FROM:
<input type="checkbox"/> TELSTRA AUTOMATED	<input checked="" type="checkbox"/> ADMIN/2/3/4/5	<input checked="" type="checkbox"/> VIRTUAL SERVER (DEDICATED) GEN1
<input checked="" type="checkbox"/> MANUAL (SUBJECT TO SLA)	<input checked="" type="checkbox"/> NETWORKADMIN	<input type="checkbox"/> VIRTUAL SERVER (DEDICATED) GEN2
<input type="checkbox"/> CUSTOMER AUTOMATED	<input type="checkbox"/> READONLY	

OVERVIEW

If you used a public or private load balancer in the past and we uplifted your vDC from Virtual Server (Dedicated) Generation 1, your old load balancer will still be running with its original configuration. You cannot directly see or control a legacy load balancer.

Virtual Server (Dedicated) Generation 1 used Cisco ACE-based load balancers. Telstra encourages you to replace them with another you can configure, control and manage yourself in a VMware NSX ESG. If you do, you can ask Telstra to remove the old one when your new load balancer is ready.

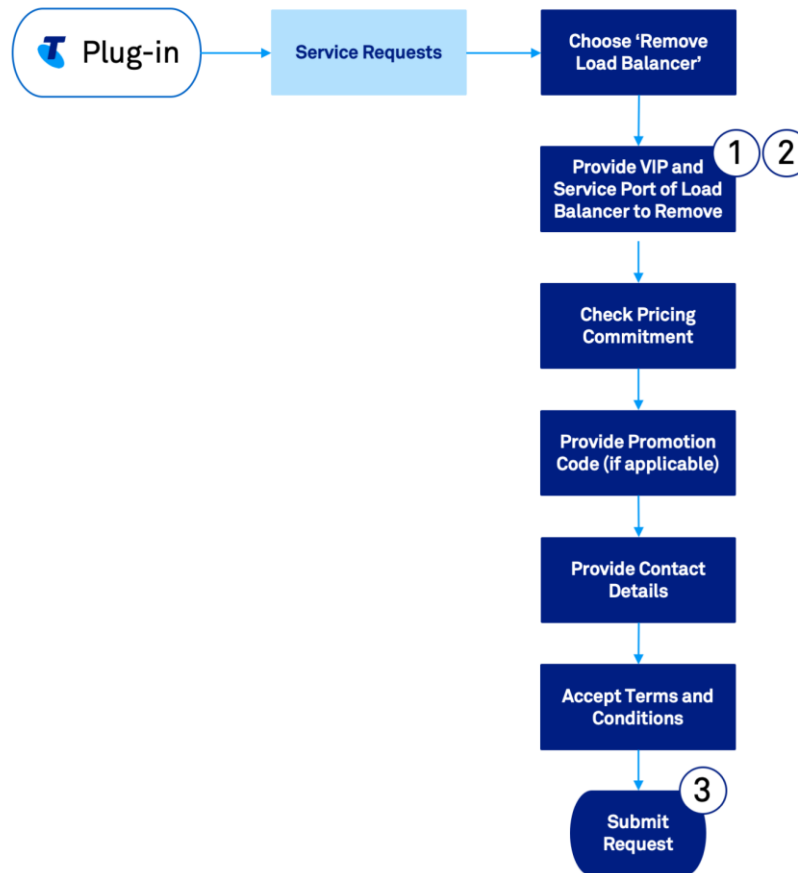
Telstra Operations may contact you submission to ask for further information or clarify your request.

PREREQUISITES

Before you can remove a load balancer:

- a. You must (still) use a legacy public or private load balancer originally provided under Virtual Server (Dedicated) Gen1
- b. You will need to know the virtual IP address and protocol port number of the load balancer you want us to remove
- c. You will need to log into the vSphere client for your vDC using an administration account.

PROCEDURE



NOTES

-
- ① The virtual IP address (VIP) is the destination IP address clients use to contact the application. It may not be the source IP address the load balancer uses to forward transactions to the application server(s) in the pool
-
- ② The service port is the destination protocol port number clients use to contact the application. It may not be the source port the load balancer uses to forward transactions to the application server(s) in the pool
-
- ③ After you submit your request, the plug-in will return a Request ID. In a future release of the plug-in, the Request ID will help you track and review your service history.
-

TASK #SR12: ADD SMTP RELAY

SERVICE LEVEL AGREEMENT	REQUIRED USER TYPE:	APPLIES TO UPLIFT FROM:
<input type="checkbox"/> TELSTRA AUTOMATED	<input checked="" type="checkbox"/> ADMIN/2/3/4/5	<input checked="" type="checkbox"/> VIRTUAL SERVER (DEDICATED) GEN1
<input checked="" type="checkbox"/> MANUAL (SUBJECT TO SLA)	<input checked="" type="checkbox"/> NETWORKADMIN	<input checked="" type="checkbox"/> VIRTUAL SERVER (DEDICATED) GEN2
<input type="checkbox"/> CUSTOMER AUTOMATED	<input type="checkbox"/> READONLY	

OVERVIEW

All outbound SMTP traffic crossing the Public Interconnect must use an approved mail relay service. The mail relay may be either inbuilt to Virtual Server (Dedicated) Gen2+ or an approved external product or service. The Public Interconnect will drop any email emanating from a domain that is not included in the inbuilt relay or sent via an approved external service.

Refer to page 46 for more information on SMTP Relay options.

This service request refers specifically to the *inbuilt* mail relay service. You do not need to submit this request for a particular domain whose traffic will pass through an approved external product or service.

Telstra Operations may contact you submission to ask for further information or clarify your request.

CONSIDERATIONS FOR ADDING AN SMTP RELAY

The inbuilt mail relay for Virtual Server (Dedicated) Gen2+ is domain-specific. It will only check and pass traffic originating from domains and sub-domains for which it is configured.

If you transmit SMTP email for several mail domains and/or sub-domains through your Public Interconnect, you must ensure that each is individually handled through an approved relay mechanism, whether inbuilt or external. It is permissible to handle one or more using the inbuilt relay and any remainders using any of the approved external mail relay services. We show examples of domain/sub-domain handling in Table 13.

SCENARIO	MAIL RELAY PLATFORM	DOMAINS	NOTES
INBUILT ONLY	Inbuilt	a.test.com.au b.test.com.au other.com	Activate using this service request
MIXED INBUILT/EXTERNAL	Inbuilt	a.test.com.au	Activate using this service request
	Internet Protection Mail	b.test.com.au other.com	Activate using Internet Protection Mail process
MIXED EXTERNAL	Internet Protection Mail	a.test.com.au	Activate using Internet Protection Mail process

SCENARIO	MAIL RELAY PLATFORM	DOMAINS	NOTES
	Microsoft Office 365	b.com.au other.com	Activate using Microsoft Office 365 process

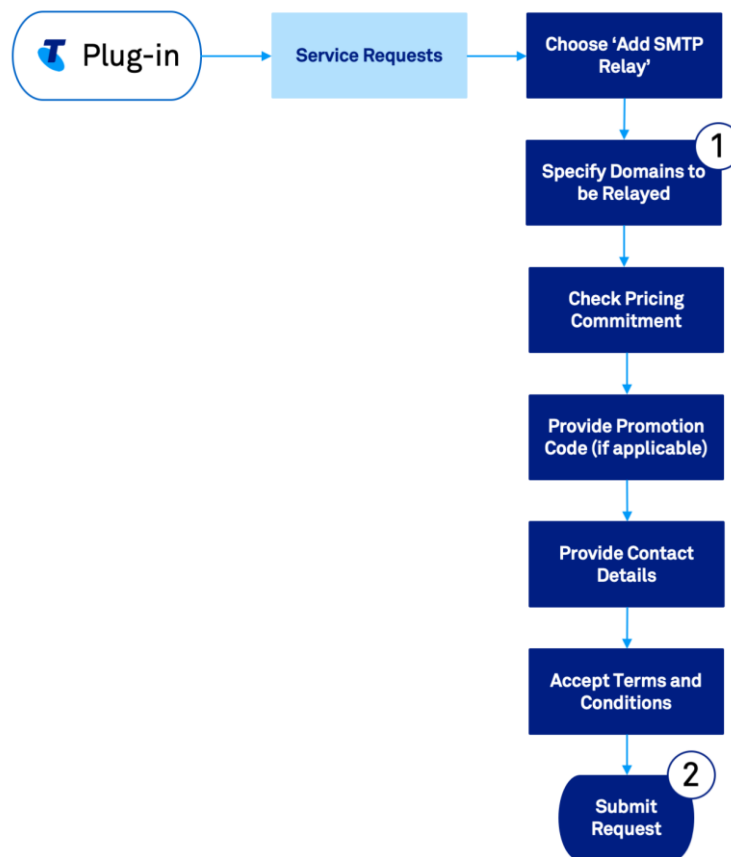
Table 13: SMTP Domain Handling

PREREQUISITES

Before you can add a domain to the inbuilt SMTP relay:

- a. You will need to log into the vSphere client for your vDC using an administration account.

PROCEDURE



NOTES

- 1 This is the mail domain to be added to the inbuilt SMTP Relay service for Virtual Server (Dedicated) Gen2+
- 2 After you submit your request, the plug-in will return a Request ID. In a future release of the plug-in, the Request ID will help you track and review your service history.

TASK #SR13: REMOVE SMTP RELAY

SERVICE LEVEL AGREEMENT	REQUIRED USER TYPE:	APPLIES TO UPLIFT FROM:
<input type="checkbox"/> TELSTRA AUTOMATED	<input checked="" type="checkbox"/> ADMIN/2/3/4/5	<input checked="" type="checkbox"/> VIRTUAL SERVER (DEDICATED) GEN1
<input checked="" type="checkbox"/> MANUAL (SUBJECT TO SLA)	<input checked="" type="checkbox"/> NETWORKADMIN	<input checked="" type="checkbox"/> VIRTUAL SERVER (DEDICATED) GEN2
<input type="checkbox"/> CUSTOMER AUTOMATED	<input type="checkbox"/> READONLY	

OVERVIEW

All outbound SMTP traffic crossing the Public Interconnect must use an approved mail relay service. The mail relay may be either inbuilt to Virtual Server (Dedicated) Gen2+ or an approved external product or service. The Public Interconnect will drop any email emanating from a domain that is not included in the inbuilt relay or sent via an approved external service.

Refer to page 46 for more information on SMTP Relay options.

This service request refers specifically to the *inbuilt* mail relay service. You do not need to submit this request for a particular domain whose traffic formerly passed through an approved external product or service.

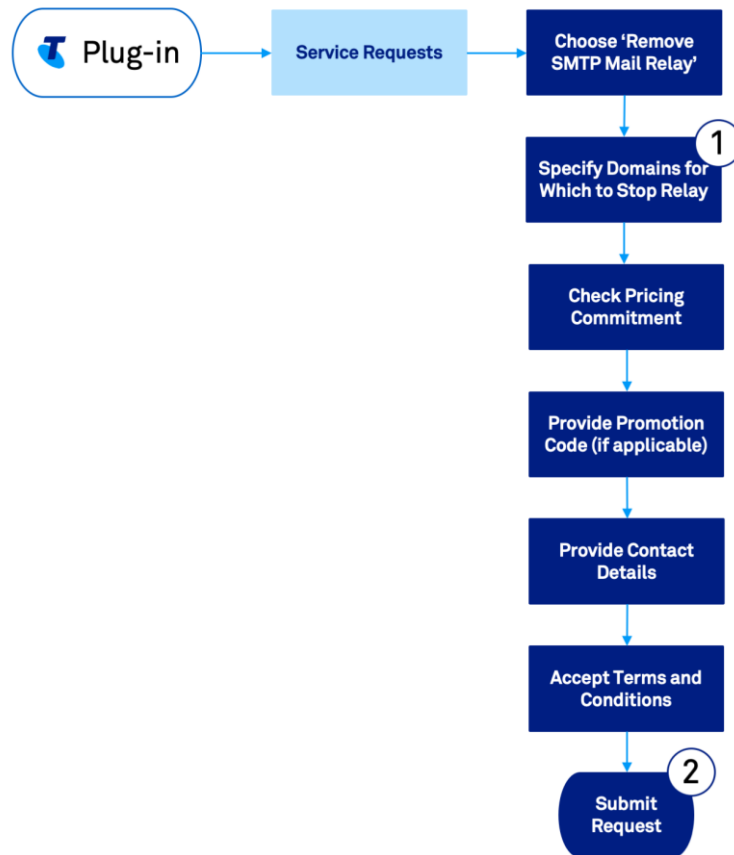
Telstra Operations may contact your submission to ask for further information or clarify your request.

PREREQUISITES

Before you can add an application to a backup:

- a. You must be an existing user of the inbuilt SMTP relay for Virtual Server (Dedicated) Gen2+
- b. You will need to log into the vSphere client for your vDC using an administration account.

PROCEDURE



NOTES

-
- 1 This is the mail domain to be removed from the inbuilt SMTP Relay service for Virtual Server (Dedicated) Gen2+
-
- 2 After you submit your request, the plug-in will return a Request ID. In a future release of the plug-in, the Request ID will help you track and review your service history.
-

TASK #SR14: CONNECT TO NEXT IP

SERVICE LEVEL AGREEMENT	REQUIRED USER TYPE:	APPLIES TO UPLIFT FROM:
<input type="checkbox"/> TELSTRA AUTOMATED	<input checked="" type="checkbox"/> ADMIN/2/3/4/5	<input checked="" type="checkbox"/> VIRTUAL SERVER (DEDICATED) GEN1
<input checked="" type="checkbox"/> MANUAL (SUBJECT TO SLA)	<input checked="" type="checkbox"/> NETWORKADMIN	<input checked="" type="checkbox"/> VIRTUAL SERVER (DEDICATED) GEN2
<input type="checkbox"/> CUSTOMER AUTOMATED	<input type="checkbox"/> READONLY	

OVERVIEW

An overwhelming proportion of Virtual Server (Dedicated) Gen1 and Gen2 customers have a private connection from their vDC to a Next IP VPN, either directly or via Cloud Gateway. Of those, most had their connection commissioned along with their vDC.

However, a connection to Next IP is not mandatory, and there is a small number of customers who do not have one when they first use their vDC.

We discuss Private Interconnections to Next IP and Cloud Gateway in depth on page 26.

You can submit this service request if you have a vDC without a Private Interconnection to a Next IP VPN and wish to establish one.

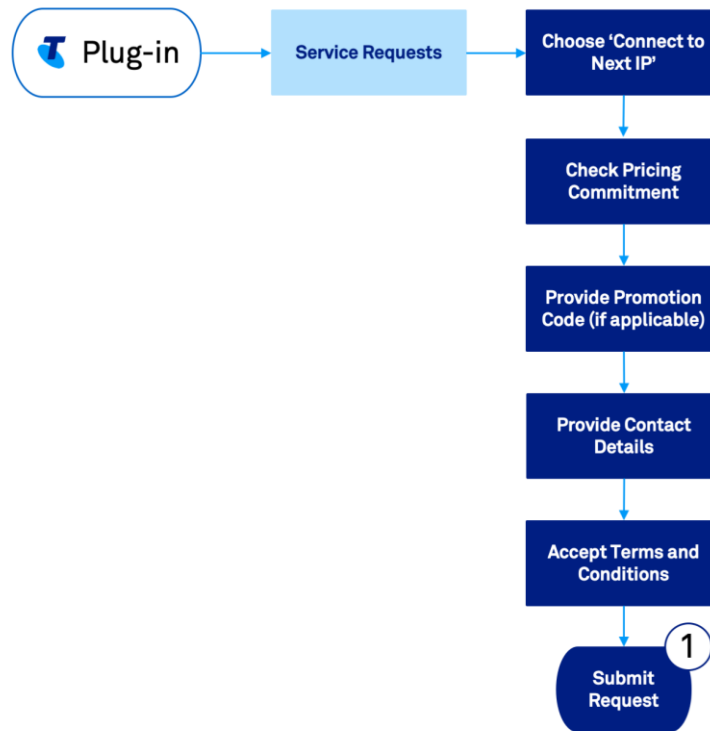
Telstra Operations may contact your submission to ask for further information or clarify your request.

PREREQUISITES

Before you can add an application to a backup:

- a. You must have a Next IP VPN
- b. You will need to log into the vSphere client for your vDC using an administration account.

PROCEDURE



NOTES

-
- 1 After you submit your request, the plug-in will return a Request ID. In a future release of the plug-in, the Request ID will help you track and review your service history.
-

TASK #SR15: IMPORT DATA

SERVICE LEVEL AGREEMENT	REQUIRED USER TYPE:	APPLIES TO UPLIFT FROM:
<input type="checkbox"/> TELSTRA AUTOMATED	<input checked="" type="checkbox"/> ADMIN/2/3/4/5	<input checked="" type="checkbox"/> VIRTUAL SERVER (DEDICATED) GEN1
<input checked="" type="checkbox"/> MANUAL (SUBJECT TO SLA)	<input checked="" type="checkbox"/> NETWORKADMIN	<input checked="" type="checkbox"/> VIRTUAL SERVER (DEDICATED) GEN2
<input type="checkbox"/> CUSTOMER AUTOMATED	<input type="checkbox"/> READONLY	

OVERVIEW

You may occasionally need to shift a large amount of data (hundreds of GB or several TB) into Virtual Server (Dedicated) Gen2+. However, your access bandwidth into your Next IP VPN or to the Internet may cause the migration to take hours or days. Moreover, the movement of the data over your access links may adversely affect the performance of your other applications.

You can import data using out-of-band means instead. After you submit this request and we clarify your requirements, Telstra will mail a NAS device to you on loan. At the time of writing, we have 3TB and 18TB devices available. Upon receipt, you load it with your data and return it to us using pre-paid postage. When we receive it, we install in one of our storage arrays and make it available to your vDC as a CIFS share you can mount in any of your VMs.

CONSIDERATIONS FOR DATA IMPORT

When you receive the NAS device and connect it to your local network, you will have the option to mount it using NFS or CIFS/SMB/Samba. You can then load the it with your data (at LAN-equivalent rates) and return it to us.

After we receive and re-install the NAS device in our storage farm, we make it available to you as a CIFS share. The share can only be reached from your vDC and is protected by username and password.

Refer to the Pricing Guide for further information on Telstra's charges for this service.

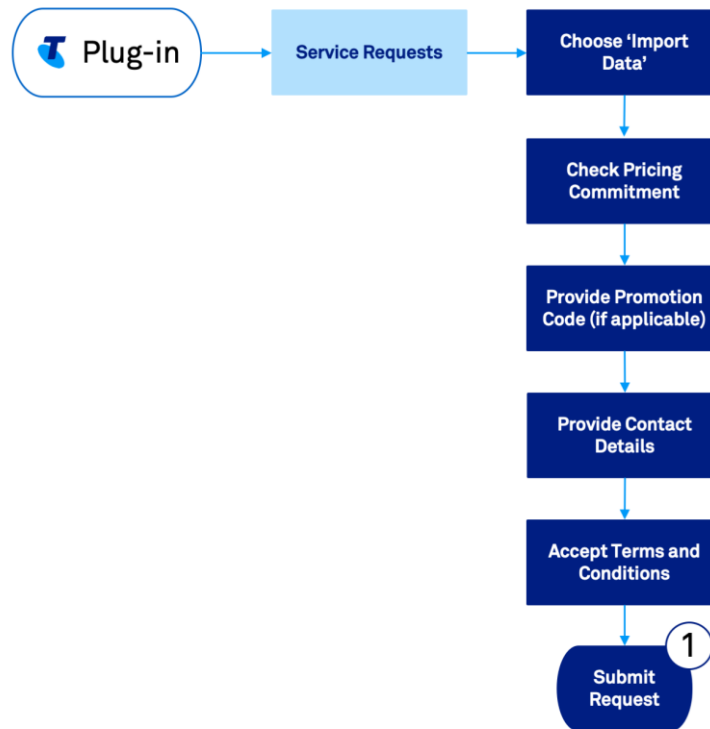
Telstra Operations may contact you submission to ask for further information or clarify your request.

PREREQUISITES

Before you can add an application to a backup:

- a. You will need to log into the vSphere client for your vDC using an administration account.

PROCEDURE



NOTES

-
- ① After you submit your request, the plug-in will return a Request ID. In a future release of the plug-in, the Request ID will help you track and review your service history.
-

TASK #SR16: EXPORT DATA

SERVICE LEVEL AGREEMENT	REQUIRED USER TYPE:	APPLIES TO UPLIFT FROM:
<input type="checkbox"/> TELSTRA AUTOMATED	<input checked="" type="checkbox"/> ADMIN/2/3/4/5	<input checked="" type="checkbox"/> VIRTUAL SERVER (DEDICATED) GEN1
<input checked="" type="checkbox"/> MANUAL (SUBJECT TO SLA)	<input checked="" type="checkbox"/> NETWORKADMIN	<input checked="" type="checkbox"/> VIRTUAL SERVER (DEDICATED) GEN2
<input type="checkbox"/> CUSTOMER AUTOMATED	<input type="checkbox"/> READONLY	

OVERVIEW

You may occasionally need to shift a large amount of data (hundreds of GB or several TB) out of Virtual Server (Dedicated) Gen2+. However, your access bandwidth into your Next IP VPN or to the Internet may cause the migration to take hours or days. Moreover, the movement of the data over your access links may adversely affect the performance of your other applications.

You can export data using out-of-band means instead. After you submit this request and we clarify your requirements, we allocate you a NAS device in one of our storage arrays and make it available to your vDC as a CIFS share you can mount in any of your VMs. At the time of writing, we have 3TB and 18TB devices available.

After you load it with the export data, Telstra will de-commission the device and mail it to you. Upon receipt, you can extract your data and return the device to us using pre-paid postage.

CONSIDERATIONS FOR DATA IMPORT

When we allocate the NAS device in our storage farm, we make it available to you as a CIFS share. The share can only be reached from your vDC and is protected by username and password.

When you receive the NAS device and connect it to your local network, you will have the option to mount it using NFS or CIFS/SMB/Samba. You can then extract your data (at LAN-equivalent rates) and return the device to us when completed.

Refer to the Pricing Guide for further information on Telstra's charges for this service.

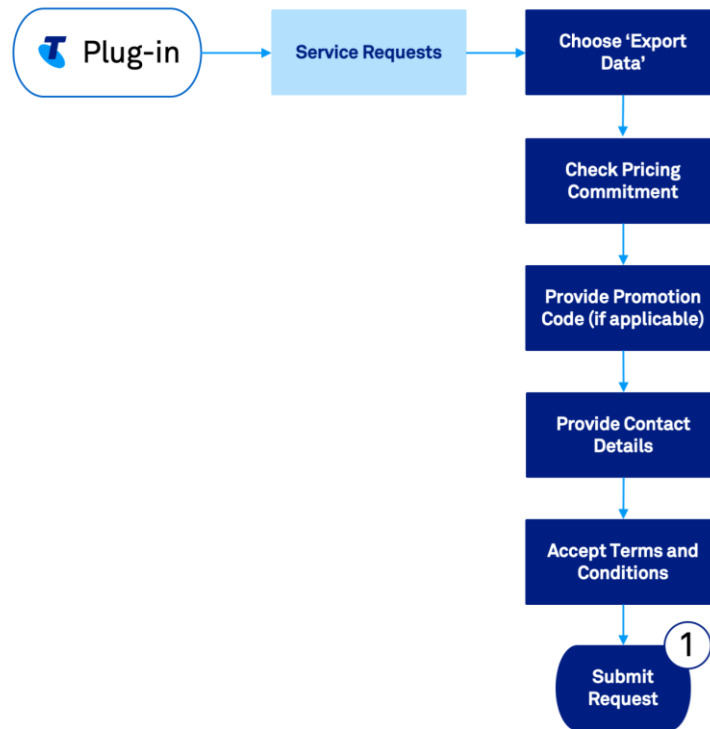
Telstra Operations may contact you submission to ask for further information or clarify your request.

PREREQUISITES

Before you can add an application to a backup:

- a. You must be an existing customer of TMB
- b. You will need to log into the vSphere client for your vDC using an administration account.

PROCEDURE



NOTES

1

After you submit your request, the plug-in will return a Request ID. In a future release of the plug-in, the Request ID will help you track and review your service history.

TASK #SR17: UPDATE ACCOUNT CONTACT DETAILS

SERVICE LEVEL AGREEMENT

- TELSTRA AUTOMATED
- MANUAL (SUBJECT TO SLA)
- CUSTOMER AUTOMATED

REQUIRED USER TYPE:

- ADMIN/2/3/4/5
- NETWORKADMIN
- READONLY

APPLIES TO UPLIFT FROM:

- VIRTUAL SERVER (DEDICATED) GEN1
- VIRTUAL SERVER (DEDICATED) GEN2

OVERVIEW

For each vDC, Telstra records the details of the person we contact by default if there is a commercial or other account issue with your tenancy, or we need to communicate with you for some unforeseen reason.

You can submit this service request to change the details of the default account contact person.

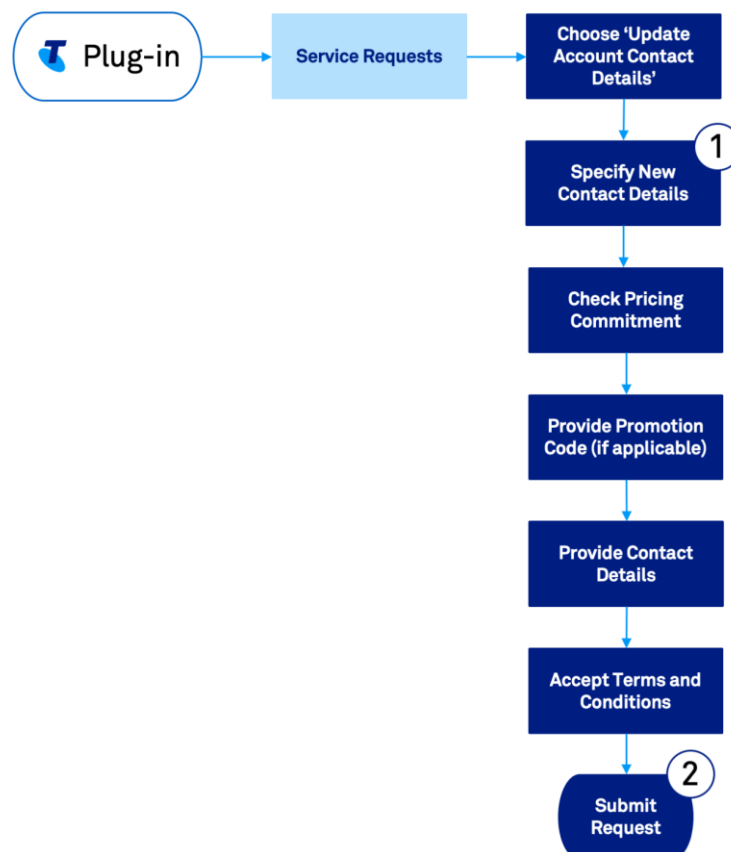
Telstra Operations may contact you submission to ask for further information or clarify your request.

PREREQUISITES

Before you can add an application to a backup:

- a. You will need to log into the vSphere client for your vDC using an administration account.

PROCEDURE



NOTES

- ① The new account contact details include the person's name, mobile number and/or office number and an email address
 - ② After you submit your request, the plug-in will return a Request ID. In a future release of the plug-in, the Request ID will help you track and review your service history.
-

TASK #SR18: UPDATE TECHNICAL CONTACT DETAILS

SERVICE LEVEL AGREEMENT	REQUIRED USER TYPE:	APPLIES TO UPLIFT FROM:
<input type="checkbox"/> TELSTRA AUTOMATED	<input checked="" type="checkbox"/> ADMIN/2/3/4/5	<input checked="" type="checkbox"/> VIRTUAL SERVER (DEDICATED) GEN1
<input checked="" type="checkbox"/> MANUAL (SUBJECT TO SLA)	<input checked="" type="checkbox"/> NETWORKADMIN	<input checked="" type="checkbox"/> VIRTUAL SERVER (DEDICATED) GEN2
<input type="checkbox"/> CUSTOMER AUTOMATED	<input type="checkbox"/> READONLY	

OVERVIEW

For each vDC, Telstra records the details of the person we contact by default if there is a technical issue with your tenancy.

You can submit this service request to change the details of the default technical contact person.

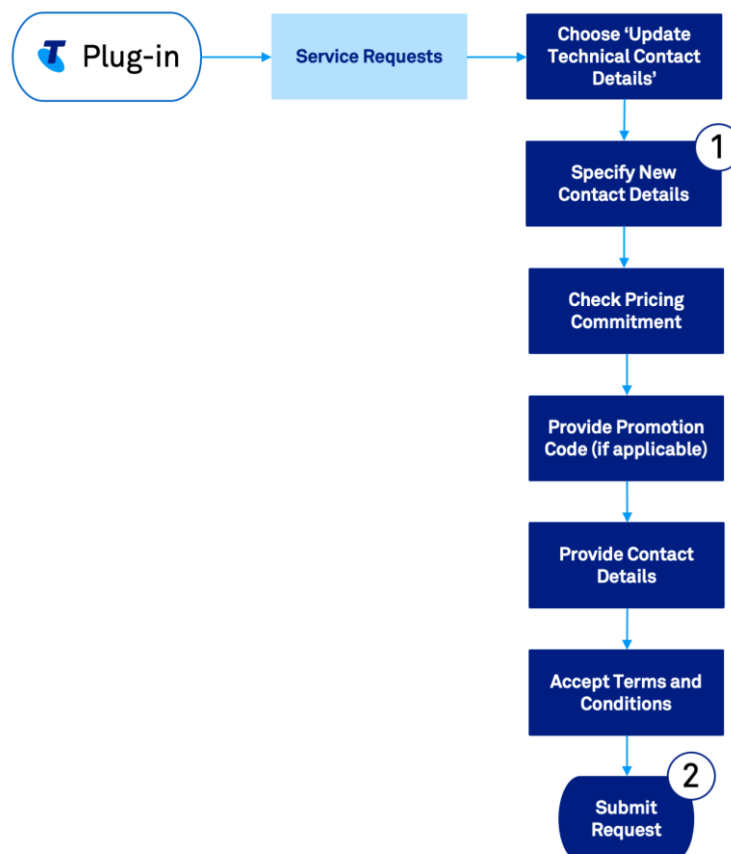
Telstra Operations may contact you submission to ask for further information or clarify your request.

PREREQUISITES

Before you can add an application to a backup:

- a. You will need to log into the vSphere client for your vDC using an administration account.

PROCEDURE



NOTES

- ① The new technical contact details include the person's name, mobile number and/or office number and an email address
 - ② After you submit your request, the plug-in will return a Request ID. In a future release of the plug-in, the Request ID will help you track and review your service history.
-

TASK #SR19: SUBMIT A NON-SPECIFIC SERVICE REQUEST

SERVICE LEVEL AGREEMENT

- TELSTRA AUTOMATED
- MANUAL (SUBJECT TO SLA)
- CUSTOMER AUTOMATED

REQUIRED USER TYPE:

- ADMIN/2/3/4/5
- NETWORKADMIN
- READONLY

APPLIES TO UPLIFT FROM:

- VIRTUAL SERVER (DEDICATED) GEN1
- VIRTUAL SERVER (DEDICATED) GEN2

OVERVIEW

You can submit this service request for changes or issues not covered by any other Plug-in option.

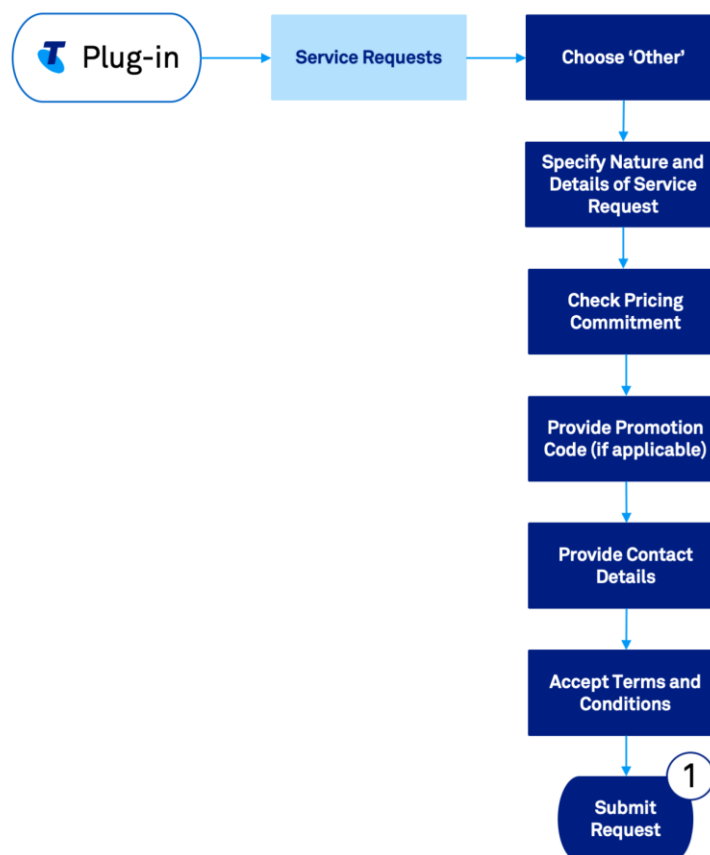
Telstra Operations may contact your submission to ask for further information or clarify your request.

PREREQUISITES

Before you can add an application to a backup:

- a. You will need to log into the vSphere client for your vDC using an administration account.

PROCEDURE



NOTES

- 1 After you submit your request, the plug-in will return a Request ID. In a future release of the plug-in, the Request ID will help you track and review your service history.
-

Chapter 15

NSX TASKS

TASK #NS01: ADD A LOGICAL SWITCH

SERVICE LEVEL AGREEMENT	REQUIRED USER TYPE:	APPLIES TO UPLIFT FROM:
<input type="checkbox"/> TELSTRA AUTOMATED	<input type="checkbox"/> ADMIN/2/3/4/5	<input checked="" type="checkbox"/> VIRTUAL SERVER (DEDICATED) GEN1
<input type="checkbox"/> MANUAL (SUBJECT TO SLA)	<input checked="" type="checkbox"/> NETWORKADMIN	<input checked="" type="checkbox"/> VIRTUAL SERVER (DEDICATED) GEN2
<input checked="" type="checkbox"/> CUSTOMER AUTOMATED	<input type="checkbox"/> READONLY	

PURPOSE

To create a logical Layer-2 segments over which VMs, DLRs and/or ESGs can communicate directly with each other.

OVERVIEW

As you construct your vDC topology, you may need to create new, separate logical Layer-2 broadcast domains or segments. NSX calls these entities **Logical Switches**. You can use a logical switch in a flat, multi-tier or multi-zone topology, or as a stub connected to an ESG. It supports public or private IP address ranges.

NSX maps the logical switch to a unique VXLAN. You can then attach interfaces from VMs, DLRs and/or ESGs to the segment and apply addresses to them from an IP subnet.

We show an example of a complex multi-tier topology in Figure 16. This example uses several Logical Switches to provide connections between resources in different levels of the topological hierarchy.

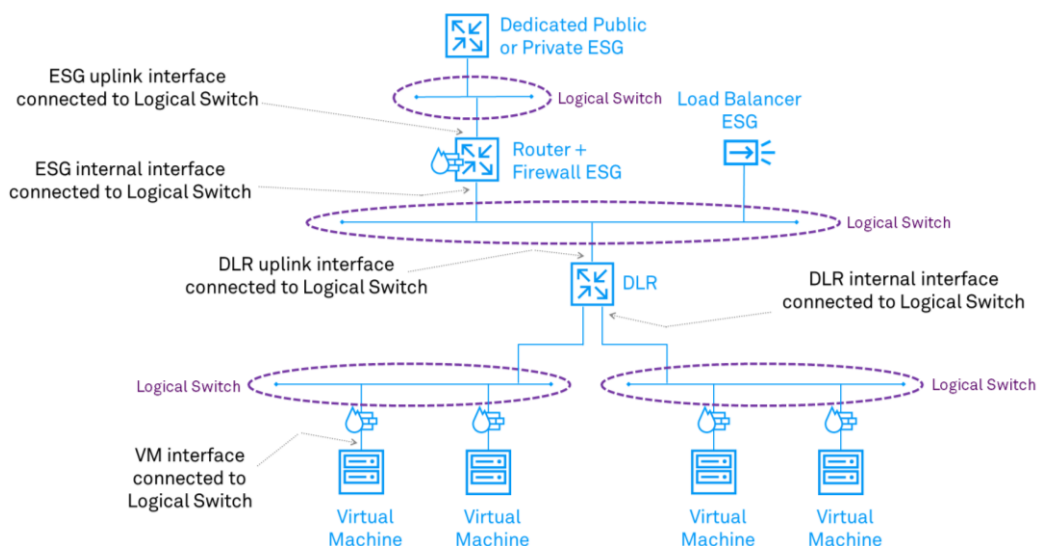


Figure 16: Using a Logical Switch to Connect Resources

CONFIGURATION TIPS



You can administer and define Logical switches under *Networking and Security* in vSphere.

When we built or uplifted your vDC, Telstra may have configured one or more Logical Switches to connect your resources. The names of the Logical Switches we created will generally follow one of two templates:

Type 1 – used for segments supporting system functions

```
<service ID>-<location>-<seq_a>-sth-<seq_b>-VRHA
```

Type 2 – used for general connectivity between your resources:

```
<IP range>_<mask>-<role>-<service ID>
```

Examples are:

```
9620081-flin-01-sth-01-VRHA
```

```
10.11.20.0_24-pri-9620081
```

You should not change the configuration of Logical Switches used for system functions (ie. Type 1). While rarely if ever necessary, you might occasionally decide to edit the configuration of Logical Switches we have previously built for general connectivity in your vDC (Type 2).

When you create a Logical Switch or edit its configuration, Telstra offers these recommendations:

- 1 You may name your new Logical Switch according to your own standards. You can also re-name pre-built Type 2 Logical Switches to suit your standards. We recommend you do not alter or rename Type 1 Logical Switches
- 2 You should usually accept all default configuration settings. These will be suitable for the vast majority of Logical Switches. In particular, you should not change the Replication Mode, which will default to Unicast
- 3 You will only see one choice of Transport Zone. Telstra created this Transport Zone when we provisioned or uplifted your vDC. While you will have the capability to create more Transport Zones using NSX, it is unnecessary
- 4 After you create your Logical Switch, you will populate it with interfaces from each member entity (VM, DLR and/or ESG) that will use it for direct communication.

INFORMATION RESOURCES

You can learn more about Logical Switches by referring to these VMware Docs:

- [Logical Switch Concepts](#)
- [How to Add a Logical Switch](#)
- [How to Connect a Logical Switch to an NSX Edge \(ESG or DLR\)](#)
- [How to Connect Virtual Machines to a Logical Switch](#)

TASK #NS02: ADD AN EDGE SERVICES GATEWAY

SERVICE LEVEL AGREEMENT	REQUIRED USER TYPE:	APPLIES TO UPLIFT FROM:
<input type="checkbox"/> TELSTRA AUTOMATED	<input type="checkbox"/> ADMIN/2/3/4/5	<input checked="" type="checkbox"/> VIRTUAL SERVER (DEDICATED) GEN1
<input type="checkbox"/> MANUAL (SUBJECT TO SLA)	<input checked="" type="checkbox"/> NETWORKADMIN	<input checked="" type="checkbox"/> VIRTUAL SERVER (DEDICATED) GEN2
<input checked="" type="checkbox"/> CUSTOMER AUTOMATED	<input type="checkbox"/> READONLY	

PURPOSE

To build a new ESG in your vDC to deliver specific routing, security, load balancing, NAT, VPN, DHCP and/or DNS functions.

OVERVIEW

An NSX Edge Services Gateway (ESG) is a virtual appliance that can undertake several important functions. Apart from its static and dynamic routing features, an ESG can include a firewall, load balancer, NAT gateway, VPN concentrator, DHCP server, DHCP relay and/or DNS server. ESGs support HA active/standby configurations running over dual VM appliances.

Edge Services Gateways are integral components Virtual Server (Dedicated) Gen2+. Telstra builds a Dedicated Private ESG and a Dedicated Public ESG when we either provision or uplift each vDC.

As you construct your vDC topology, you may need to create additional ESGs because you want to implement some or all of the features we mentioned above.

We show a multi-level topology using two customer-defined ESGs in Figure 17. One ESG acts as a router and firewall while the other implements a load balancer. We have only separated these functions for illustrative purposes and it is quite possible to perform all of them in a single ESG.

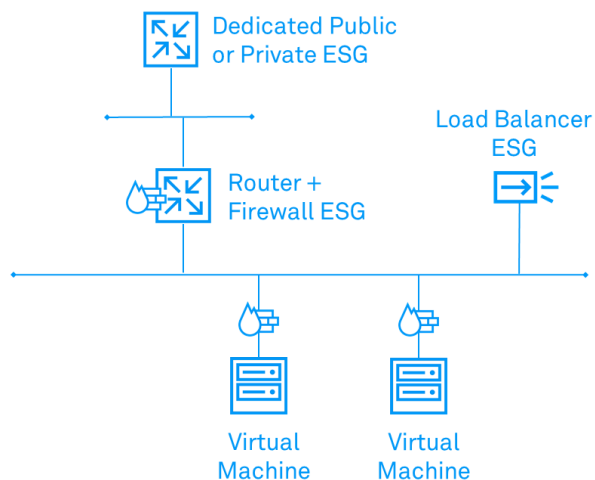


Figure 17: Edge Services Gateways in Multi-Level Topologies

When you create an ESG, you must choose the size of the underlying VM appliance from options offered by NSX. VMware provides guidelines in VMware Docs to help you choose the correct size.

CONFIGURATION TIPS



You can administer and define ESGs under *Networking and Security* in vSphere.

When we built or uplifted your vDC, Telstra will have configured two ESGs:

- a. The Dedicated Public ESG
- b. The Dedicated Private ESG.

After we complete the uplift, you can see both ESGs and inspect or change their configurations, but you need to be careful because you can disrupt their connectivity external networks and resources if you make a mistake or try to configure a feature or setting we do not support. We have published advice and rules elsewhere in this User Guide that describe routing behaviours between the Dedicated Public and Dedicated Private ESGs and the Public and Private Interconnects.

When you create your own ESG or edit an ESG's configuration, Telstra offers these recommendations:

- 1 You may name your new ESG according to your own standards. You can also re-name ESGs. However, we recommend that you do not rename the Dedicated Private ESG or Dedicated Public ESG because this could affect our assurance activities and our ability to meet our SLAs
- 2 Where you choose to activate a specific function, you will find the default values are quite suitable much of the time. Possible exceptions are:
- 3 You may wish to enable a default firewall policy
- 4 You might need to adjust the HA settings if your ESG is particularly critical
- 5 As a further guideline to sizing your ESG, we use Quad Large VM appliances when Telstra we build your Dedicated Public ESG and Dedicated Private ESG
- 6 You are free to incorporate HA active/standby VM appliances underneath your ESG
- 7 When you nominate a datastore to hold the VM system files, ensure you choose one of the correct type (Active, Performance or Ultra) and with sufficient space to hold your files
- 8 If you plan to connect the ESG to new Logical Switch, be sure to create the Logical Switch before the ESG.

INFORMATION RESOURCES

You can learn more about ESGs and how to use them in Virtual Server (Dedicated) Gen2+by referring to these VMware Docs:

- [Routing using VMware NSX](#)
- [How to add an Edge Services Gateway](#) (includes choosing the correct size of underlying VM appliance)
- [NSX Edge configuration](#)
- [How to Connect a Logical Switch to an NSX Edge \(ESG or DLR\)](#)

TASK #NS03: ADD DISTRIBUTED LOGICAL ROUTER

SERVICE LEVEL AGREEMENT	REQUIRED USER TYPE:	APPLIES TO UPLIFT FROM:
<input type="checkbox"/> TELSTRA AUTOMATED	<input type="checkbox"/> ADMIN/2/3/4/5	<input checked="" type="checkbox"/> VIRTUAL SERVER (DEDICATED) GEN1
<input type="checkbox"/> MANUAL (SUBJECT TO SLA)	<input checked="" type="checkbox"/> NETWORKADMIN	<input checked="" type="checkbox"/> VIRTUAL SERVER (DEDICATED) GEN2
<input checked="" type="checkbox"/> CUSTOMER AUTOMATED	<input type="checkbox"/> READONLY	

PURPOSE

To build a new DLR in your vDC to perform basic traffic routing among VMs spread over a number of Logical Switches

OVERVIEW

An NSX Distributed Logical Router (DLR) is a virtual router primarily intended for east-west routing between VMs on different segments. A DLR is sometimes called a Logical (Distributed) Router in VMware documentation.

By using a DLR, you may avoid the need to route traffic through an ESG further up the topological hierarchy when there are no local security or other functional implications to consider.

While VMware classes both as NSX Edge devices, a DLR is simpler and contains fewer features than an ESG. If we use an analogy from classic networking, you might think of each of them this way:

- An ESG is similar to a WAN access router: it contains fewer interfaces but often exhibits many features beyond routing, such as security, traffic management, relay and server functions, and remote access
- A DLR is more like a Layer-3 LAN switch: it can contain many interfaces and can quickly route between ports or segments but is unlikely to match a fully-functioned router for features.

VMware describes a number of important rules and considerations when you wish to use a DLR. Refer to VMware Docs for more information.

We show an example of multi-level topology that incorporates a DLR in Figure 18. The DLR connects to one interface on an ESG acting as a router and firewall. This helps to protect the networks south of the DLR but facilitates northbound communication according to establish firewall rules.

Unlike an ESG, you do not choose the size of the underlying VM appliance supporting a DLR. VMware provides a default appliance configuration as you define the new DLR. However, you must still specify the cluster and datastore that will house the DLR VM appliance and its files.

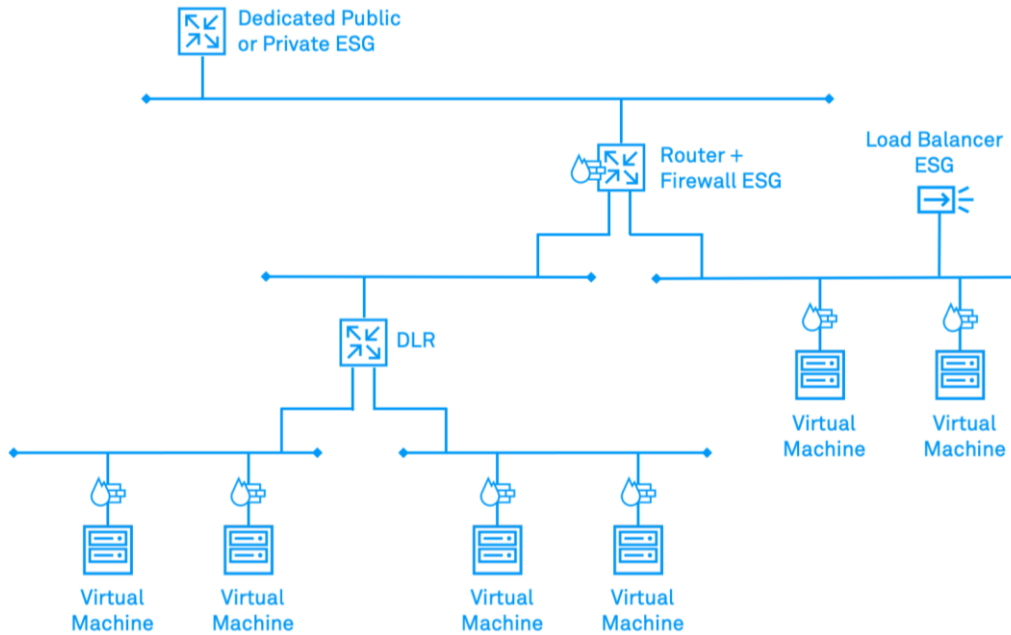


Figure 18: Using a DLR in a Complex Topology

CONFIGURATION TIPS



You can administer and define DLRs under *Networking and Security* in vSphere.

When you create your own DLR, Telstra offers these recommendations:

- 1 You may name your new DLR according to your own standards
- 2 You will find the default values for configuration parameters are quite suitable much of the time. However, you might need to adjust the HA settings if your DLR is particularly critical
- 3 You are free to incorporate HA active/standby VM appliances underneath your DLR
- 4 When you nominate a datastore to hold the VM system files, ensure you choose one of the correct type (Active, Performance or Ultra) and with sufficient space to hold your files
- 5 If you plan to connect the DLR to new Logical Switch, be sure to create the Logical Switch before the DLR.

INFORMATION RESOURCES

You can learn more about DLRs and how to use them in Virtual Server (Dedicated) Gen2+by referring to these VMware Docs:

- [Routing using VMware NSX](#)
- [How to add a Logical \(Distributed\) Router](#) (includes choosing the correct size of underlying VM appliance)
- [NSX Edge configuration](#)
- [How to Connect a Logical Switch to an NSX Edge \(ESG or DLR\)](#)

TASK #NS04: CONNECT A VM TO A LOGICAL SWITCH

SERVICE LEVEL AGREEMENT	REQUIRED USER TYPE:	APPLIES TO UPLIFT FROM:
<input type="checkbox"/> TELSTRA AUTOMATED	<input type="checkbox"/> ADMIN/2/3/4/5	<input checked="" type="checkbox"/> VIRTUAL SERVER (DEDICATED) GEN1
<input type="checkbox"/> MANUAL (SUBJECT TO SLA)	<input checked="" type="checkbox"/> NETWORKADMIN	<input checked="" type="checkbox"/> VIRTUAL SERVER (DEDICATED) GEN2
<input checked="" type="checkbox"/> CUSTOMER AUTOMATED	<input type="checkbox"/> READONLY	

PURPOSE

To join a VM interface to an existing logical Layer-2 segment so it can communicate directly with other VMs, DLRs and/or ESGs.

OVERVIEW

NSX supports logical Layer-2 broadcast domains based on the VXLAN protocol. Each segment is called a **Logical Switch** and is mapped to a unique VXLAN. You can use a logical switch in a flat, multi-tier or multi-zone topology, or as a stub connected to an ESG and/or DLR. It supports public or private IP address ranges.

A Logical Switch will have no members at the time you create it. You will need to subsequently add each member of the Logical Switch by specifying the entity (VM, ESG or DLR) and interface to use.

Moreover, as you manage your vDC topology, you may need to modify the membership of your Logical Switch and attach additional members to it.

CONFIGURATION TIPS



You can administer and define Logical switches under *Networking and Security* in vSphere.

Telstra will have built some of your Logical Switches when we provisioned or uplifted your vDC. You may have since added more. You should not need to change the configuration or membership of Logical Switches we created for system functions, but you might occasionally decide to edit the configuration or membership of Logical Switches used for general connectivity in your vDC, regardless of who built them.

To add a VM to the membership of your Logical Switch, you can highlight the Logical Switch in your vSphere client and use 'Add VM' from the *Actions* drop-down menu.

(You can detach a VM from the Logical Switch using the same method but choosing 'Remove VM' instead.)

INFORMATION RESOURCES

You can learn more about adding a VM to a Logical Switch by referring to these VMware Docs:

- [Logical Switch Concepts](#)
- [How to Add a Logical Switch](#)
- [How to Connect Virtual Machines to a Logical Switch](#)

TASK #NS05: CONNECT AN ESG OR DLR TO A LOGICAL SWITCH

SERVICE LEVEL AGREEMENT	REQUIRED USER TYPE:	APPLIES TO UPLIFT FROM:
<input type="checkbox"/> TELSTRA AUTOMATED	<input type="checkbox"/> ADMIN/2/3/4/5	<input checked="" type="checkbox"/> VIRTUAL SERVER (DEDICATED) GEN1
<input type="checkbox"/> MANUAL (SUBJECT TO SLA)	<input checked="" type="checkbox"/> NETWORKADMIN	<input checked="" type="checkbox"/> VIRTUAL SERVER (DEDICATED) GEN2
<input checked="" type="checkbox"/> CUSTOMER AUTOMATED	<input type="checkbox"/> READONLY	

PURPOSE

To join an ESG or DLR interface to an existing logical Layer-2 segment so it can communicate directly with other VMs, DLRs and/or ESGs.

OVERVIEW

NSX supports logical Layer-2 broadcast domains based on the VXLAN protocol. Each segment is called a **Logical Switch** and is mapped to a unique VXLAN. You can use a logical switch in a flat, multi-tier or multi-zone topology, or as a stub connected to an ESG and/or DLR. It supports public or private IP address ranges.

A Logical Switch will have no members at the time you create it. You will need to subsequently add each member of the Logical Switch by specifying the entity (VM, ESG or DLR) and interface to use.

Moreover, as you manage your vDC topology, you may need to modify the membership of your Logical Switch and attach additional members to it.

CONFIGURATION TIPS



You can administer and define Logical switches under *Networking and Security* in vSphere.

Telstra will have built some of your Logical Switches when we provisioned or uplifted your vDC. You may have since added more. You should not need to change the configuration or membership of Logical Switches we created for system functions, but you might occasionally decide to edit the configuration or membership of Logical Switches used for general connectivity in your vDC, regardless of who built them.

To add an ESG or DLR to the membership of your Logical Switch, you can highlight the Logical Switch in your vSphere client and use 'Connect Edge' from the *Actions* drop-down menu.

INTERFACE COUNT IMPACTS

VMware limits the number of internal, uplink and/or trunk interfaces per ESG to a total of 10. If you use internal interfaces to connect a Logical Switch to your ESG, each VXLAN will consume 1 internal interface. But, if you use trunk interfaces on your ESG, you can connect multiple Logical Switches to a single trunk interface and thereby improve scalability.

Hence, Telstra recommends that you use trunk interfaces rather than internal interfaces to attach Logical Switches to your ESGs.

INFORMATION RESOURCES

You can learn more about adding an ESG or DLR to a Logical Switch by referring to these VMware Docs:

- [*Logical Switch Concepts*](#)
- [*How to Add a Logical Switch*](#)
- [*How to Connect a Logical Switch to an NSX Edge \(ESG or DLR\)*](#)
- [*Configure an Interface*](#)

TASK #NS06: MODIFY NSX FIREWALL

SERVICE LEVEL AGREEMENT	REQUIRED USER TYPE:	APPLIES TO UPLIFT FROM:
<input type="checkbox"/> TELSTRA AUTOMATED	<input type="checkbox"/> ADMIN/2/3/4/5	<input checked="" type="checkbox"/> VIRTUAL SERVER (DEDICATED) GEN1
<input type="checkbox"/> MANUAL (SUBJECT TO SLA)	<input checked="" type="checkbox"/> NETWORKADMIN	<input checked="" type="checkbox"/> VIRTUAL SERVER (DEDICATED) GEN2
<input checked="" type="checkbox"/> CUSTOMER AUTOMATED	<input type="checkbox"/> READONLY	

PURPOSE

To adjust the stateful firewall inspection (SFI) characteristics of traffic flowing through a vDC. Those characteristics include sections, objects and groups, and their governing rules.

OVERVIEW

The NSX Firewall is a logical resource that can inspect traffic flowing through your vDC. It is a composite logical device that consists of the Distributed Firewall (DFW) and Edge Firewalls. You can collate and aggregate your vDC objects and rules using a variety of criteria and characteristics that may make administration smoother and may even automatically adapt to your configuration changes.

Once we uplift your vDC, you have management control over your NSX Firewall and are responsible for the logical security of your vDC. Whenever you change your vDC topology or configuration, you should assess its effects on your NSX Firewall and make appropriate changes to continue to meet your security policy and protect your resources. This might include supplementing your NSX Firewall with further security products and services that you purchase from us or acquire through other means.

We discuss the impact of the uplift process on the way you may configure and use your NSX Firewall on page 36.

CONFIGURATION TIPS



You can administer the NSX Firewall under *Networking and Security* in vSphere.

Your NSX Firewall will already exist when you first login to your vDC after we complete our uplift process. It will follow a common template consisting of:

- Any custom rules you have previously specified for your private topology and resources
- Any custom rules you have previously specified for your public topology and resources
- Default (catch-all) rules we have added for your private topology and resources
- Default (catch-all) rules we have added for your public topology and resources
- Default rules added by NSX.

The NSX Firewall offers you a significant degree of configuration flexibility. While this makes it powerful and adaptable, you must apply sufficient rigour and care to your definitions of objects, groups and policy rules. If you do not, you risk introducing policy conflicts that either admit undesirable traffic to your vDC or block legitimate communication. Such conflicts can be hard to locate and resolve, particularly if you have not noticed them immediately and/or your configuration has grown organically over time.

INFORMATION RESOURCES

You can learn more about the NSX Firewall, including the DFW and Edge Firewalls by referring to these VMware Docs:

- [*Logical Firewall*](#)
- [*Distributed Firewall*](#)
- [*Edge Firewall*](#)
- [*Working with Firewall Rule Sections*](#)
- [*Working with Firewall Rules*](#)

TASK #NS07: ADD L2 VPN

SERVICE LEVEL AGREEMENT	REQUIRED USER TYPE:	APPLIES TO UPLIFT FROM:
<input type="checkbox"/> TELSTRA AUTOMATED	<input type="checkbox"/> ADMIN/2/3/4/5	<input checked="" type="checkbox"/> VIRTUAL SERVER (DEDICATED) GEN1
<input type="checkbox"/> MANUAL (SUBJECT TO SLA)	<input checked="" type="checkbox"/> NETWORKADMIN	<input checked="" type="checkbox"/> VIRTUAL SERVER (DEDICATED) GEN2
<input checked="" type="checkbox"/> CUSTOMER AUTOMATED	<input type="checkbox"/> READONLY	

PURPOSE

To build a Layer-2 Stretch connection from your vDC to another location.

OVERVIEW

Layer-2 Stretch joins matched VLAN and/or VXLAN segments over an intermediate layer-3 network. It uses an NSX feature called L2 VPN that allows an ESG to act as an SSL-VPN or IPsec-VPN tunnel endpoint.

You can use Layer-2 Stretch to cross any public or private network, or a mix of them depending on the location of your facilities and your routing arrangement. This includes the Internet and your Next IP VPN.

CONFIGURATION TIPS

You can enable L2 VPN in a new purpose-built ESG or enable it in one of your existing ESGs. The way you administer L2 VPN depends on which underlying protocol you want to use. At the time of writing:

- **SSL:** you can use the vSphere Flex client to enable and configure L2 VPN
- **IPsec:** you must use the REST API to enable to configure L2 VPN
- You cannot use the vSphere HTML5 client to administer L2 VPN.

If you plan to use L2 VPN through your Public Interconnect, remember that your tunnel endpoint needs a public IP address supplied by Virtual Server (Dedicated). You cannot supply your own public IP address acquired through other means. If you plan to build a new ESG for your L2 VPN tunnel endpoint, you can apply for an additional range using Task #PA01: Add a Public IP Address (Range). Alternatively, you can consider re-using your Dedicated Public ESG, which already has a valid and suitable secondary address configured on the interface leading to the Public Interconnect.

A Layer-2 Stretch needs specific configuration settings in the logical devices that support it, such as ESGs and Logical Switches. Misconfigurations can cause looping and packet duplicates. VMware publishes L2 VPN best practices that you should follow when you build a Layer-2 Stretch service.

INFORMATION RESOURCES

You can learn more about the NSX L2 VPN by referring to these VMware Docs:

- [L2 VPN Overview](#)
- [L2 VPN Best Practices](#)
- [L2 VPN Over SSL](#)
- [L2 VPN Over IPsec](#)

TASK #NS08: ADD A LOAD BALANCER

SERVICE LEVEL AGREEMENT	REQUIRED USER TYPE:	APPLIES TO UPLIFT FROM:
<input type="checkbox"/> TELSTRA AUTOMATED	<input type="checkbox"/> ADMIN/2/3/4/5	<input checked="" type="checkbox"/> VIRTUAL SERVER (DEDICATED) GEN1
<input type="checkbox"/> MANUAL (SUBJECT TO SLA)	<input checked="" type="checkbox"/> NETWORKADMIN	<input checked="" type="checkbox"/> VIRTUAL SERVER (DEDICATED) GEN2
<input checked="" type="checkbox"/> CUSTOMER AUTOMATED	<input type="checkbox"/> READONLY	

PURPOSE

To build a public or private load balancer in your vDC.

OVERVIEW

An NSX ESG-based load balancer distributes network traffic across multiple servers. It can load-balance traffic using layer-4 and layer-7 parameters. Each approach offers advantages:

- Layer-4 load balancing is implemented at the TCP/UDP level. It is fast because it does not buffer the whole request or stub the connection, instead processing each packet header and sending it directly to the selected server
- Layer-7 load balancing is socket-based, so it creates back-to-back sessions. It receives and processes the whole request, allowing advanced traffic manipulation and DDOS mitigation. This is the default mode for TCP, HTTP and HTTPS virtual servers.

CONFIGURATION TIPS

You can enable an NSX load balancer in a new purpose-built ESG or enable it in one of your existing ESGs. In Virtual Server (Dedicated) Gen2, our provisioning policy built each Public or Private load balancer in its own ESG, but you may prefer to commission yours in the Dedicated Public or Dedicate Private ESG, according to need.

If you decide to activate your load balancer in an existing ESG, ensure you consider the impact of its processing load on the underlying VM and host. For example, you may need to alter the VM's specifications and re-deploy the ESG.

NSX load balancers offer several useful configuration features that help you make the service efficient and resilient:

- One-arm or inline mode
- Service acceleration
- SSL termination, bridging and certificate management
- Connection throttling
- Choice of:
 - Load balancing method
 - Association persistence
 - Server health monitoring

INFORMATION RESOURCES

You can learn more about NSX load balancing by referring to these VMware Docs:

- [*Logical Load Balancer*](#)
- [*Setting Up Load Balancing*](#)
- [*Managing Service Monitors*](#)
- [*Managing Server Pools*](#)
- [*Managing Virtual Servers*](#)
- [*Managing Application Rules*](#)
- [*Scenarios for NSX Load Balancer Configuration*](#)

Chapter 16

VCENTER TASKS

TASK #VM01: CREATE A VIRTUAL MACHINE

SERVICE LEVEL AGREEMENT	REQUIRED USER TYPE:	APPLIES TO UPLIFT FROM:
<input type="checkbox"/> TELSTRA AUTOMATED	<input checked="" type="checkbox"/> ADMIN/2/3/4/5	<input checked="" type="checkbox"/> VIRTUAL SERVER (DEDICATED) GEN1
<input type="checkbox"/> MANUAL (SUBJECT TO SLA)	<input type="checkbox"/> NETWORKADMIN	<input checked="" type="checkbox"/> VIRTUAL SERVER (DEDICATED) GEN2
<input checked="" type="checkbox"/> CUSTOMER AUTOMATED	<input type="checkbox"/> READONLY	

PURPOSE

Create a VM when you need a new virtual server or virtual appliance.

OVERVIEW

You can create, modify and remove VMs from the hosts and clusters in your vDC without intervention from Telstra. Each VM can host one of several different types of resources, including a virtual server or a virtual appliance such as an NSX ESG or DLR.

You can create a VM using any of these methods:

- Using a custom definition: where no other VMs in your vDC have the requirements you need (eg. OS or hardware configuration)
- Using a pre-configured VM definition: where you can export an existing VM or virtual appliance, or use a vApp stored as an OVF file
- From a VM template: where you create a master copy of a VM and then deploy multiple copies of it
- By cloning an existing VM: you can do this many times, either directly or by first cloning the existing VM to a template.

Whichever method you use, vSphere includes various ‘wizards’ that guide you through the process. The wizard will ask you to specify a name for the VM and a folder to hold it. In the past, you would put your new VM in or under a sub-folder called “Customer virtual machines” to ensure that you had the correct permissions to manage the VM. This is no longer required but you will need to prepare your intended folder in advance using the “New Folder” wizard.

CONFIGURATION TIPS

Because Virtual Server (Dedicated) is a multi-tenant architecture, you must correctly select items

When you create your VM, please observe these points and recommendations:

- 1 If you do not use a template or OVF for your new VM, it is up to you to determine the resource configuration you will need. Telstra does not provide guidance on VM sizing
- 2 You will be able to configure your VM for vMotion operation using DRS and HA
- 3 You can name your VM according to your own policies and standards
- 4 Telstra will use RBAC to restrict your ability to set parameters that may compromise the integrity or security of our multi-tenant infrastructure.

INFORMATION RESOURCES

You can learn more about VMs and how to use them in Virtual Server (Dedicated) Gen2+by referring to these VMware Docs:

- [*About vSphere Virtual Machine Administration*](#)
- [*Deploying Virtual Machines*](#)
- [*Configuring Virtual Machine Hardware*](#)
- [*Configuring Virtual Machine Options*](#)

TASK #VM02: CREATE A VM DRS GROUP

SERVICE LEVEL AGREEMENT	REQUIRED USER TYPE:	APPLIES TO UPLIFT FROM:
<input type="checkbox"/> TELSTRA AUTOMATED	<input checked="" type="checkbox"/> ADMIN/2/3/4/5	<input checked="" type="checkbox"/> VIRTUAL SERVER (DEDICATED) GEN1
<input type="checkbox"/> MANUAL (SUBJECT TO SLA)	<input type="checkbox"/> NETWORKADMIN	<input checked="" type="checkbox"/> VIRTUAL SERVER (DEDICATED) GEN2
<input checked="" type="checkbox"/> CUSTOMER AUTOMATED	<input type="checkbox"/> READONLY	

PURPOSE

To add one or more VMs to a VM DRS Group for later use in DRS VM-Host affinity rules.

OVERVIEW

If you plan to create DRS VM-Host affinity rules that influence the distribution of VMs across certain hosts, you must first arrange those respective VMs into one or more VM DRS Groups. Each VM DRS Group will consist of one or more VMs and draw its VM membership from those configured in a single host cluster.

Any given VM can be a member of more than one VM DRS Group at a time.

If you only plan to create DRS VM-VM affinity rules (ie. between individual VMs rather than between VMs and hosts) then you do not need to complete this step.

CONFIGURATION TIPS

When you create a VM DRS Group, please observe these points and recommendations:

- 1 While you can call the VM DRS Group anything you like, Telstra suggests you name it in a way that is representative of its purpose and/or its membership
- 2 If you create VM DRS Groups with overlapping memberships, you must be mindful of the way in which VMware resolves conflicts with their corresponding affinity rules

INFORMATION RESOURCES

You can learn more about DRS Groups and VM-Host affinity rules and how to use them in Virtual Server (Dedicated) Gen2+by referring to these VMware Docs:

- [Using DRS Affinity Rules](#)
- [Create a Virtual Machine DRS Group](#)
- [VM-Host Affinity Rules](#)

TASK #VM03: CREATE A HOST DRS GROUP

SERVICE LEVEL AGREEMENT	REQUIRED USER TYPE:	APPLIES TO UPLIFT FROM:
<input type="checkbox"/> TELSTRA AUTOMATED	<input checked="" type="checkbox"/> ADMIN/2/3/4/5	<input checked="" type="checkbox"/> VIRTUAL SERVER (DEDICATED) GEN1
<input type="checkbox"/> MANUAL (SUBJECT TO SLA)	<input type="checkbox"/> NETWORKADMIN	<input checked="" type="checkbox"/> VIRTUAL SERVER (DEDICATED) GEN2
<input checked="" type="checkbox"/> CUSTOMER AUTOMATED	<input type="checkbox"/> READONLY	

PURPOSE

To add one or more hosts to a Host DRS Group for later use in DRS VM-Host affinity rules.

OVERVIEW

If you plan to create DRS VM-Host affinity rules that influence the distribution of VMs across certain hosts, you must first arrange those respective hosts into one or more Host DRS Groups. Each Host DRS Group will consist of one or more hosts and draw its Host membership from those configured in a single host cluster.

Any given host can be a member of more than one Host DRS Group at a time.

If you only plan to create DRS VM-VM affinity rules (ie. between individual VMs rather than between VMs and hosts) then you do not need to complete this step.

CONFIGURATION TIPS

When you create a Host DRS Group, please observe these points and recommendations:

- 1 While you can call the Host DRS Group anything you like, Telstra suggests you name it in a way that is representative of its purpose and/or its membership
- 2 If you create Host DRS Groups with overlapping memberships, you must be mindful of the way in which VMware resolves conflicts with their corresponding affinity rules

INFORMATION RESOURCES

You can learn more about DRS Groups and VM-Host affinity rules and how to use them in Virtual Server (Dedicated) Gen2+by referring to these VMware Docs:

- [Using DRS Affinity Rules](#)
- [Create a Host DRS Group](#)
- [VM-Host Affinity Rules](#)

TASK #VM04: CREATE A VM-HOST AFFINITY RULE

SERVICE LEVEL AGREEMENT	REQUIRED USER TYPE:	APPLIES TO UPLIFT FROM:
<input type="checkbox"/> TELSTRA AUTOMATED	<input checked="" type="checkbox"/> ADMIN/2/3/4/5	<input checked="" type="checkbox"/> VIRTUAL SERVER (DEDICATED) GEN1
<input type="checkbox"/> MANUAL (SUBJECT TO SLA)	<input type="checkbox"/> NETWORKADMIN	<input checked="" type="checkbox"/> VIRTUAL SERVER (DEDICATED) GEN2
<input checked="" type="checkbox"/> CUSTOMER AUTOMATED	<input type="checkbox"/> READONLY	

PURPOSE

To configure a DRS affinity rule that specifies a relationship between a DRS Group of VMs and a DRS Group of hosts.

OVERVIEW

This task refers specifically to VM-Host rules. You can categorise each DRS VM-Host affinity rule as either *required* ('must') or *preferential* ('should').

When DRS distributes VMs across a cluster of hosts, it will attempt to honour all your affinity rules. However, sometimes it cannot fulfil the affinity conditions because of conflicting rules or a lack of available resources. This is called an *affinity violation*. vSphere reports affinity violations and the reason(s) they have occurred under 'Faults' in the DRS monitoring panel.

CONFIGURATION TIPS

DRS VM-Host affinity rules apply to VMs and hosts in groups. You need to create your designated groups of each before you configure VM-Host affinity or anti-affinity rules. Refer to:

- Task #VM02: Create a VM DRS GROUP
- Task #VM03: Create a Host DRS GROUP

When you create a DRS VM-Host affinity rule, please observe these points and recommendations:

- 1 While your vSphere administrative permissions and the way we configure your host clusters can shape your degree of control over certain DRS and HA behaviours, you will generally have access to the full range of DRS affinity rules
- 2 While you can call the DRS VM-Host affinity rules anything you like, Telstra suggests you name it in a way that is representative of its purpose and/or its membership
- 3 If you create DRS VM-Host or VM-VM affinity rules with conflicting specifications or conditions that cannot be met with the resources available to DRS, you must be mindful of the order and method in which VMware deals with them and how you can check for affinity violations
- 4 Our section on DRS Affinity Rules on page 43 discusses rule conflicts and affinity violations and that they may affect our background maintenance and support activities in your vDC. It also outlines our suggestions when you decide to implement or change DRS Affinity for yourself.

INFORMATION RESOURCES

You can learn more about DRS Affinity and how to use it in Virtual Server (Dedicated) Gen2+by referring to these VMware Docs:

- [Using DRS Affinity Rules](#)
- [VM-Host Affinity Rules](#)

TASK #VM05: CREATE A VM-VM AFFINITY RULE

SERVICE LEVEL AGREEMENT

- TELSTRA AUTOMATED
- MANUAL (SUBJECT TO SLA)
- CUSTOMER AUTOMATED

REQUIRED USER TYPE:

- ADMIN/2/3/4/5
- NETWORKADMIN
- READONLY

APPLIES TO UPLIFT FROM:

- VIRTUAL SERVER (DEDICATED) GEN1
- VIRTUAL SERVER (DEDICATED) GEN2

PURPOSE

To configure a DRS affinity rule that determines how vMotion places a two of more VMs across hosts in a DRS cluster.

OVERVIEW

This task refers specifically to VM-VM affinity rules.

When DRS distributes VMs across a cluster of hosts, it will attempt to honour all your affinity rules. However, sometimes it cannot fulfil the affinity conditions because of conflicting rules or a lack of available resources. This is called an *affinity violation*. vSphere reports affinity violations and the reason(s) they have occurred under 'Faults' in the DRS monitoring panel.

CONFIGURATION TIPS

You can nominate the VMs for your DRS VM-VM affinity or anti-affinity rule as you configure it. You do not need to define VM Groups in advance.

When you create a DRS VM-VM affinity or anti-affinity rule, please observe these points and recommendations:

- 1 While your vSphere administrative permissions and the way we configure your host clusters can shape your degree of control over certain DRS and HA behaviours, you will generally have access to the full range of DRS affinity rules
- 2 While you can call the DRS VM-VM affinity and anti-affinity rules anything you like, Telstra suggests you name it in a way that is representative of its purpose and/or its membership
- 3 If you create DRS VM-VM and VM-Host affinity rules with conflicting specifications or conditions that cannot be met with the resources available to DRS, you must be mindful of the order and method in which VMware deals with them and how you can check for affinity violations
- 4 Our section on DRS Affinity Rules on page 43 discusses rule conflicts and affinity violations and that they may affect our background maintenance and support activities in your vDC. It also outlines our suggestions when you decide to implement or change DRS Affinity for yourself.

INFORMATION RESOURCES

You can learn more about DRS Affinity and how to use it in Virtual Server (Dedicated) Gen2+by referring to these VMware Docs:

- [Using DRS Affinity Rules](#)
- [VM-VM Affinity Rules](#)