Town of Caledon – Disaster Recovery Playbook

System: Administration Building Data Centre

Role (Key Stakeholders)	Name	Email	Phone
Owner	Ankur Arora	Ankur.Arora@caledon.ca	xxx-xxx-xxxx
Approver			
Contributor (Technical)			
Contributor (DBA)			
Contributor (Network)			
Contributor (Vendor)			

Document Control

Document creation and edit records should be maintained by the Town’s disaster recovery coordinator (DRC) or business continuity manager (BCM).

Document Name	
Version	
Date Created	
Date Last Modified	
Last Modified By	

Document Change History

Version	Date	Description	Approval

Contact Information

This section will list the Town’s internal IT contacts along with external service providers (if applicable). This is the team that will conduct ongoing disaster recovery operations for this service, along with

Town Contact	Title	Phone	Email
Service Provider Contact	Role	Phone	Email

Data Centre Access Control List

Maintain an up-to-date access control list (ACL) specifying who, within the Town and any service partners, has access to the data centre and resources herein.

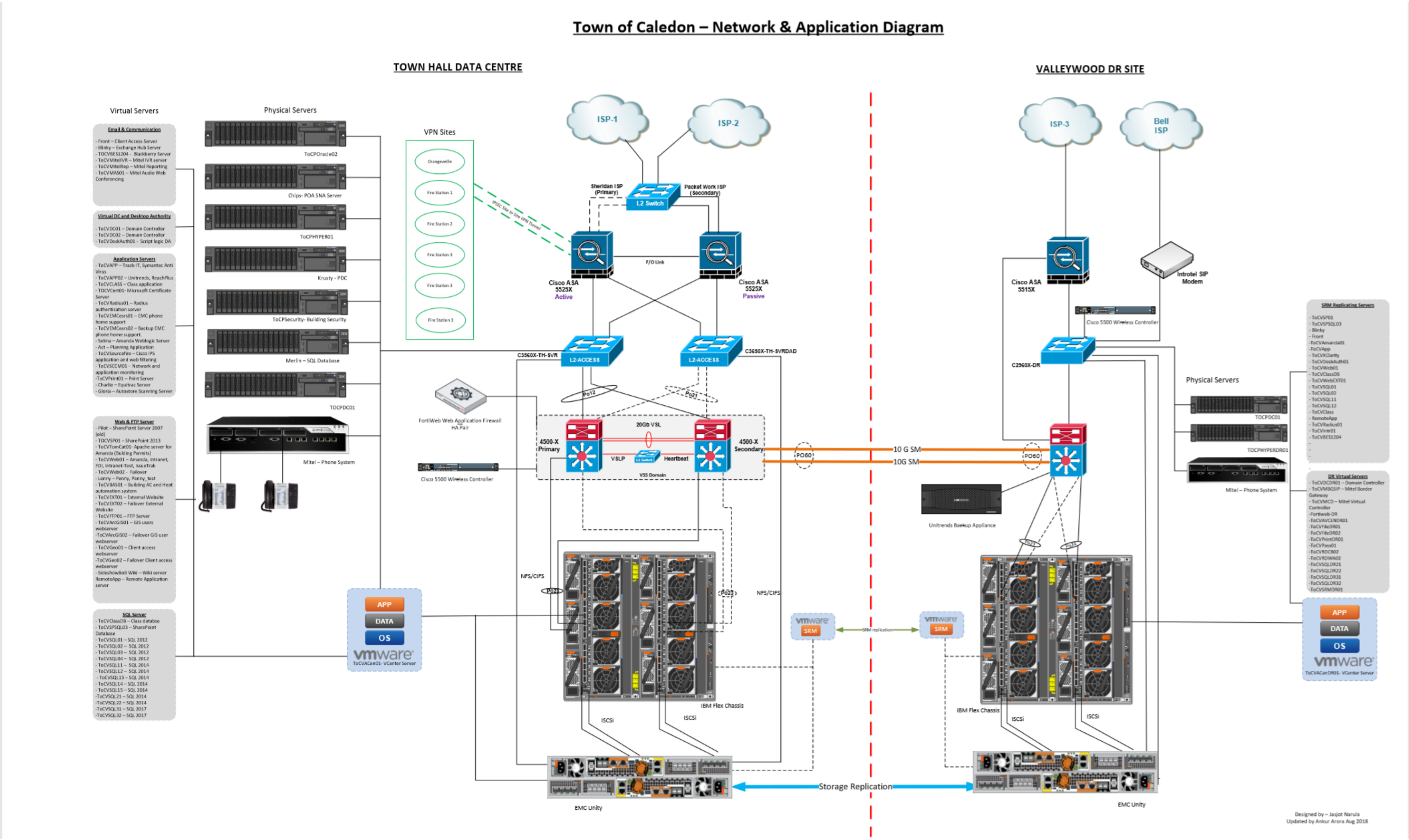
Be sure to specify which individuals can introduce guests to the data centre. This is required for determining, in the event of an emergency, who may be the designated point person for facilitating access to critical infrastructure. During a recovery event, the Town's primary operations team will be involved in system recovery, making contact and data centre access information critical to the success of the recovery process.

Name	Role	Contact Info	Access Level

Part 2 – System Level Procedures

Data Centre Recovery

Infrastructure Overview – Primary Data Centre (Administration Building) & DR Site (Snelcrest Drive)



Town of Caledon – Network & Application Diagram

TOWN HALL DATA CENTRE

Virtual Servers

Email & Communication

- Front – Client Access Server
- Blinky – Exchange Hub Server
- TOCVBES1204 - Blackberry Server
- ToCVMitelIVR – Mitel IVR server
- ToCVMitelRep – Mitel Reporting
- ToCVMAS01 – Mitel Audio Web Conferencing

Virtual DC and Desktop Authority

- ToCVDC01 – Domain Controller
- ToCVDC02 – Domain Controller
- ToCVDeskAuth01 - Script logic DA

Application Servers

- ToCVAPP – Track-IT, Symantec Anti Virus
- ToCVAPP02 – Unitrends, ReachPlus
- ToCVCLASS – Class application
- TOCVCert01- Microsoft Certificate Server
- ToCVRadius01 – Radius authentication server
- ToCVEMCesrs01 – EMC phone home support
- ToCVEMCesrs02 – Backup EMC phone home support.
- Selma – Amanda Weblogic Server
- Act – Planning Application
- ToCVSourcefire – Cisco IPS application and web filtering
- ToCVSCCM01 - Network and application monitoring
-ToCVPrint01 – Print Server
- Charlie – Equitrac Server
- Gloria – Autostore Scanning Server

Web & FTP Server

- Pilot – SharePoint Server 2007 (old)
- TOCVSP01 – SharePoint 2013
- ToCVTomCat01- Apache server for Amanda (Bulding Permits)
- ToCVWeb01 – Amanda, Intranet, FOI, Intranet-Test, IssueTrak
- ToCVWeb02 - Failover
- Lenny – Penny, Penny_test
- ToCVBAS01 – Building AC and Heat automation system
- ToCVEXT01 – External Website
- ToCVEXT02 – Failover External Website
- ToCVFTP01 – FTP Server
- ToCVArcGIS01 – GIS users webserver
-ToCVArcGIS02 – Failover GIS user webserver
- ToCVGeo01 – Client access webserver
-ToCVGeo02 – Failover Client access webserver
- SideshowBoB Wiki – Wiki server
RemoteApp – Remote Application server

SQL Server

- ToCVClassDB – Class databse
- ToCVSPSQL03 – SharePoint Database
- ToCVSQL01 – SQL 2012
- ToCVSQL02 – SQL 2012
- ToCVSQL03 – SQL 2012
- ToCVSQL04 – SQL 2012
- ToCVSQL11 – SQL 2014
- ToCVSQL12 – SQL 2014
- ToCVSQL13 – SQL 2014
- ToCVSQL14 – SQL 2014
- ToCVSQL15 – SQL 2014
-ToCVSQL21 – SQL 2014
-ToCVSQL22 – SQL 2014
-ToCVSQL31 – SQL 2017
-ToCVSQL32 – SQL 2017

VALLEYWOOD DR SITE

SRM Replicating Servers

- ToCVSP01
- ToCVSPSQL03
- Blinky
- Front
-ToCVAmanda01
-ToCVApp
- ToCVXClarity
- ToCVDeskAuth01
- ToCVWeb01
- ToCVClassDB
- ToCVWebEXT01
- ToCVSQL01
- ToCVSQL02
- ToCVSQL11
- ToCVSQL12
- ToCVClass
- RemoteApp
- ToCVRadius01
- ToCVIntr01
- ToCVBES1204
-
-
-
-

DR Virtual Servers

- ToCVDCDR01 – Domain Controller
- ToCVMBGSIP – Mitel Border Gateway
- ToCVMCD – Mitel Virtual Controller
-Fortiweb-DR
-ToCVAVCENDR01
-ToCVFileDR01
-ToCVFileDR02
-ToCVPrintDR01
-ToCVPass01
-ToCVRDCB02
-ToCVRDWA02
-ToCVSQLDR21
-ToCVSQLDR22
-ToCVSQLDR31
-ToCVSQLDR32
-ToCVSRMDR01

Order of Restoration Table – Core Infrastructure & IT Business Systems

This table assumes all items listed as “active” in **Appendix A – DR Site Current State** are enabled and require no intervention by the recovery team.

This section includes instructions for recovery personnel that lay out which infrastructure components to restore and in which order. It should take into account application dependencies, authentication, middleware, database and third-party elements and list restoration items by system or service type. Ensure this order of restoration in understood before engaging in recovery activities.

Task #	Activity (*business system)	System/Service Description	Notes
1	Assemble Recovery Team	Ensure that the required recovery team members have been contacted	Refer to “Contact Information” in Section 1 of this document
2	Secure Internet	Move to a location with Internet access	Recovery team must secure a corporate laptop with a configured VPN client
6	VPN Testing	Test VPN access to DR site	Must be on a corporate laptop. Please refer to **Appendix D – VPN Access**
5	Primary DC Shutdown	Perform a soft shutdown of the primary DC	Refer to **Appendix C – Primary DC Shutdown**
7	Telephony (VOIP)	Automatic failover of corporate phones	Refer to **Appendix E – VOIP Testing**
8	Email Testing	Exchange 2010 standard	Refer to **Appendix F – Email Testing**
9	Database Recovery	Oracle & SQL database recovery	Refer to **Appendix G – Database Recovery**
10	File/Print Recovery	Desktop Authority (Quest) & Print Server	Refer to **Appendix H – File and Print Recovery**
3	Physical Infrastructure Checklist	Review physical infrastructure checklist to ensure availability of services	Refer to **Appendix B –DR Infrastructure Checklist** (items 1-11)
4	Core Infrastructure Services Checklist	Ensure core infrastructure services are active	Refer to **Appendix B – DR Infrastructure Checklist** (items 15-18)
11	Helpdesk Recovery	TrackIT	Refer to **Appendix I – Helpdesk System Recovery**
12	*GIS Recovery		Refer to **Appendix J – GIS System Recovery**

Appendix A – DR Site Current State

Appendix B – DR Infrastructure Checklist

Current State			🟩 active 🟨 warning 🟥 issue
Item#	**Description**	**Status**	**Notes**
Physical Infrastructure			
Facilities (power, cooling, space)			
1	Power	🟩	Generator – natural gas (Enbridge) – May affect major power outage due to close proximity (22km) from Town Hall. There has been power spikes in the past
2	Cooling	🟩	Could be an issue with cooling
3	Fire Suppression	🟥	Does not exist at DR site
4	Space	🟩	Adequate
5	Access	🟨	Need to clarify who actually has access to the facility (IT Infrastructure) – Does database team? (No) Need a list of names. Facilities group also has access to the room. Door code for access (may want to review). AA
Resource Layers (network – routers/switches/firewalls, storage – SAN/NAS/DAS, compute – physical servers/hosts)			
6	Switches (2)	🟩	Cisco 4500x, Cisco 2960x Document steps to confirm connectivity
7	Firewall (1)	🟩	Cisco 5515x Document steps to confirm connectivity
8	Backup Appliance	🟩	Unitrends Document steps to confirm connectivity
9	Server Chassis	🟩	IBM Flex Chassis (5 nodes) 5 x VMware Hosts
10	Physical Servers (2)	🟩	IBM (need model number) (HyperV 2012 host + Windows 2016 DC)
11	SAN	🟩	EMC Unity – 80TB(RAW) – 60TB usable (Ankur to provide details)
Software-Defined			
12	VMware (SRM)	🟩	Total 20 servers (25 licenses) Replication schedule – every 5 minutes
13	Virtual servers (16)	🟨	VMware v6.5 (Gary to add server details) (RDS, load-balancer, phone system) some of these servers are live. There are production servers running within this environment that need to be identified.

Current State			active 🟩 warning 🟨 issue 🟥
Item#	Description	Status	Notes
14	Oracle VM (2)	🟨	HyperV 2012 – (passive). Replication from production. Manual activation required **NOTE:** licensing only permits 10-days of activity in DR site
Core Infrastructure Services (DNS/DHCP/Security/Password Management)			
15	DNS (AD integrated)	🟩	Running on a physical server and also virtual server (live today). May be a delay at TOD (propagation)
16	DHCP	🟨	Running on a virtual server (in production today for about 30% of addressing) Can it handle 100%? (Yes). Has not been tested (active/active)
17	Password Management	🟩	In production - no work necessary at TOD
18	Internet	🟩	Will be available
Essential Infrastructure Services (Authentication/AD/File&Priint/Apps/DB/Remote Access/Internet/Monitoring/MDM/Backup)			
19	Authentication	🟩	Domain Controller is currently active (1 VM + 1 Physical)
20	Remote Access (VPN)	🟩	
21	SQL	🟥	Requires Database team to recover (SRM)
22	Oracle	🟥	Requires Database team to recover (SRM)
23	File/Print	🟥	
IT Business Services (Helpdesk/VOIP/Email/GIS/Reporting/Project Management/Development Services)			
24	Helpdesk	🟥	TrackIT – fat client - DB is replicating (SQL)
25	GIS	🟥	TBD
26	Email	🟥	Exchange 2010 Standard (5 Databases) Recovered via SRM

Current State	active	warning	issue

Item#	Description	Status	Notes
27	VOIP (phone system)	🟨	Should failover but this needs to be tested
28	External Websites (5)	🟥	Hosted by third-party + internal (not currently replicated)
29	Reporting	🟥	
30	Project Management	🟥	
31	Development	🟥	

Appendix C – Primary DC Shutdown

Primary Datacenter Shutdown Steps

Note: This section assumes you have the ability to connect to the Primary DC through the DR site network VPN connection. Depending on the scenario a site visit and/or modification of the steps in this section may be required.

In a partial disaster scenario (e.g. a power outage threat). There may be a need to shutdown the Primary DC. Below is the order and steps to shut down the critical components.

VMs → Hosts → Chassis & Physical Servers → SAN

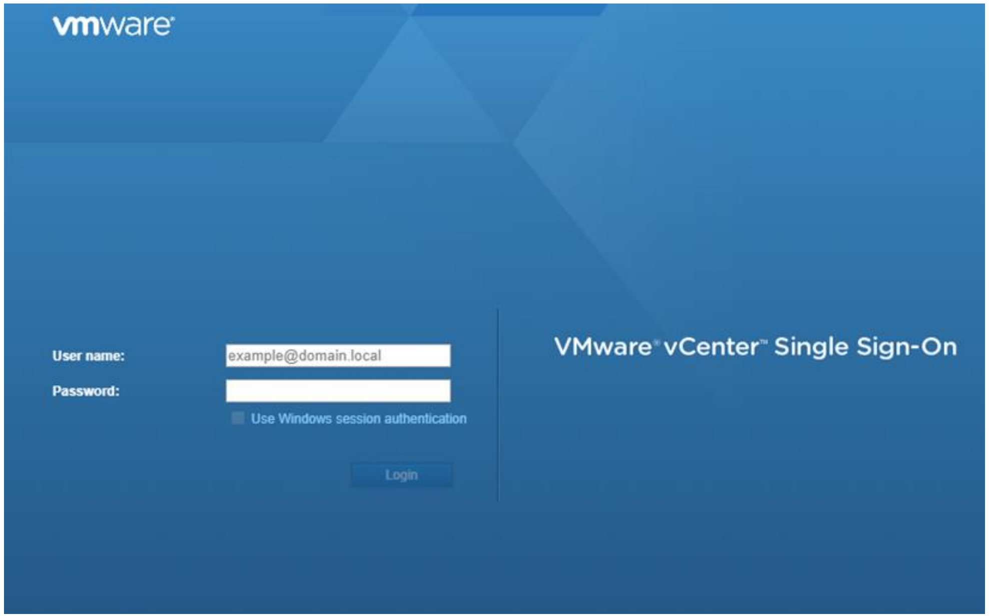
*Networking gear doesn't need to be shutdown

<u>VMware Recovery Steps</u>

1. Open a web browser and browse to https://tocvavcen01

2. Click on vSphere Web Client (Flash)

3. Login with your Domain Admin account



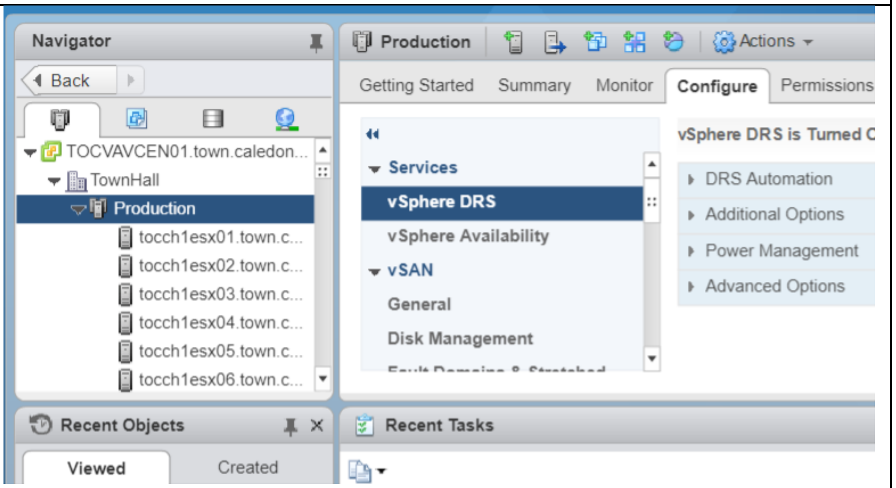
User name: example@domain.local

Password:

□ Use Windows session authentication

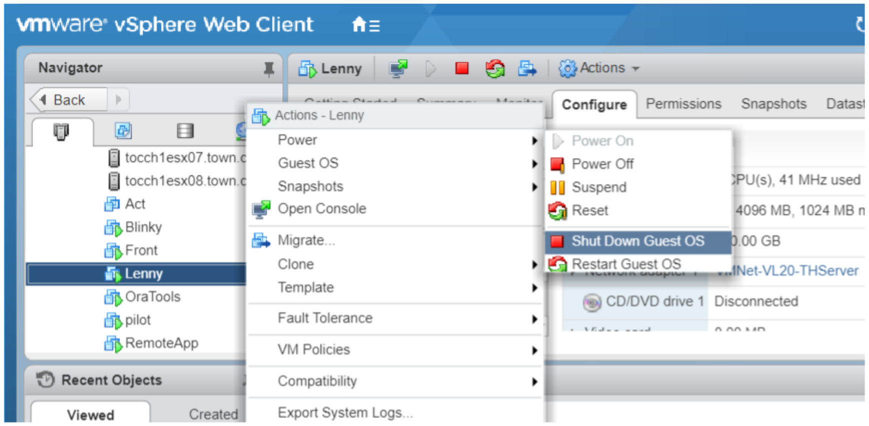
Primary Datacenter Shutdown Steps (continued)

4. Expand the **Production** Cluster under **Host and Clusters**



5. Right click the VM you wish to shutdown and select Power then click Shut Down Guest OS

Important: Make a note of VMs that are already shutdown as they won't need to be powered on when bringing the VMs back online at the Primary DC.

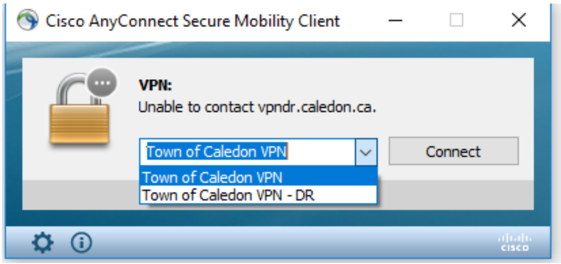


Appendix D – VPN Access

VPN Access Recovery Steps

VPN access to the Town of Caledon Network requires a corporate laptop. If not on-site at DR or Town Hall you will need establish the VPN connection via the DR site firewall.

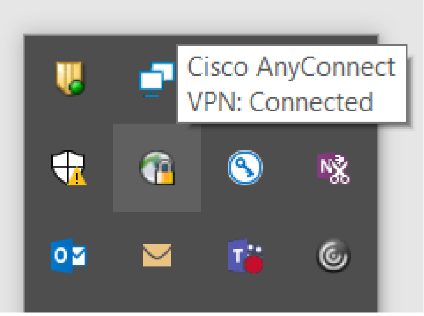
1. From the corporate laptop Go to the Start Menu to search and launch “Cisco AnyConnect Secure Mobility Client”.
2. Once launched select “Town of Caledon – DR” from the drop down.



Cisco AnyConnect Secure Mobility Client

VPN:
Unable to contact vpndr.caledon.ca.

1. Click Connect and enter your username and password.
2. Confirm you are Connected by hovering the mouse pointer over the AnyConnect icon in the system tray.



Cisco AnyConnect
VPN: Connected

Note: If unable to establish a VPN connection to the DR site firewall:

-Confirm internet connectivity

-Confirm local firewall is not blocking a VPN connection

If still unable to connect – a visit to the DR site would be required to troubleshoot further. Once on-site steps in Appendix L and M can be used for reference

Appendix E – VOIP Testing

Appendix F – Email Testing

Appendix G – Database Recovery

Appendix H – File and Print Recovery

Appendix I – Helpdesk Recovery

Appendix J – GIS Recovery