



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.

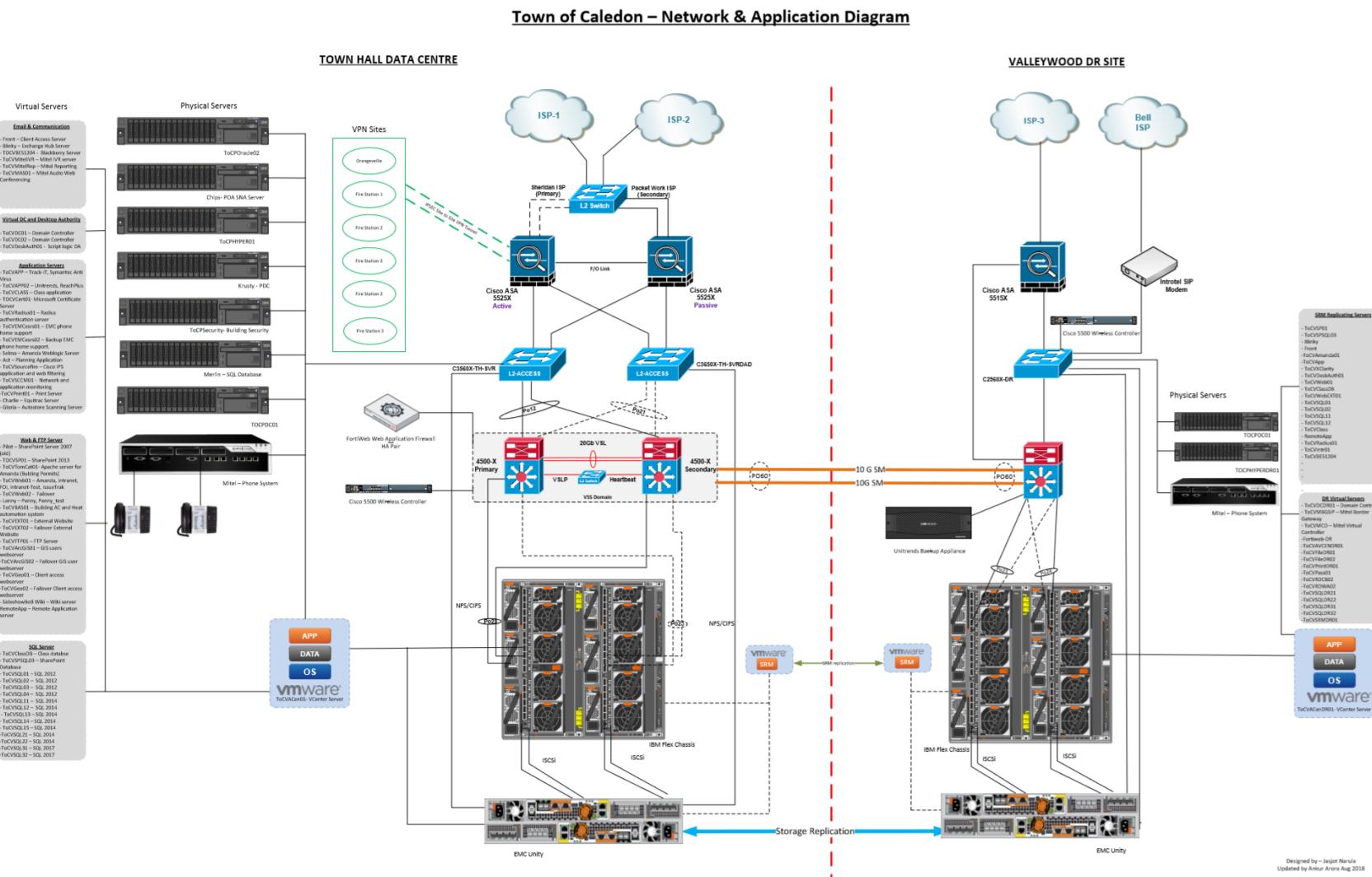
Be sure to specify which individuals can introduce guests to the data centre. This is required for determining, in the event of an emergency, who may be the designated point person for facilitating access to critical infrastructure. During a recovery event, the Town's primary operations team will be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



Designed by = Jaijai Narula
Updated by Ankur Arora Aug 2018

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 is 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 |
| 3 | VPN Testing | Test VPN access to DR site | Must be on a corporate laptop. Please refer to Appendix D – VPN Access |
| 4 | Primary DC Shutdown | Perform a soft shutdown of the primary DC | Refer to Appendix C – Primary DC Shutdown |
| 5 | Telephony (VOIP) | Automatic failover of corporate phones | Refer to Appendix E – VOIP Testing |
| 6 | Email Testing | Exchange 2010 standard | Refer to Appendix F – Email Testing |
| 7 | Database Recovery | Oracle & SQL database recovery | Refer to Appendix G – Database Recovery |
| 8 | File/Print Recovery | Desktop Authority (Quest) & Print Server | Refer to Appendices H/I – File and Print Recovery |
| 9 | Physical Infrastructure Checklist | Review physical infrastructure checklist to ensure availability of services | Refer to Appendix B – DR Infrastructure Checklist (items 1-11) |
| 10 | 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 J – Helpdesk System Recovery |
| 12 | *GIS Recovery | | Refer to Appendix K – 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 | Green | 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 | Green | Could be an issue with cooling | | | |
| 3 | Fire Suppression | Red | Does not exist at DR site | | | |
| 4 | Space | Green | Adequate | | | |
| 5 | Access | Yellow | 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) | Green | Cisco 4500x, Cisco 2960x Document steps to confirm connectivity | | | |
| 7 | Firewall (1) | Green | Cisco 5515x Document steps to confirm connectivity | | | |
| 8 | Backup Appliance | Green | Unitrends Document steps to confirm connectivity | | | |
| 9 | Server Chassis | Green | IBM Flex Chassis (5 nodes) 5 x VMware Hosts | | | |
| 10 | Physical Servers (2) | Green | IBM (need model number) (HyperV 2012 host + Windows 2016 DC) | | | |
| 11 | SAN | Green | EMC Unity – 80TB(RAW) – 60TB usable (Ankur to provide details) | | | |
| Software-Defined | | | | | | |
| 12 | VMware (SRM) | Green | Total 20 servers (25 licenses) Replication schedule – every 5 minutes | | | |
| 13 | Virtual servers (16) | Yellow | 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) | Yellow | 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) | Green | Running on a physical server and also virtual server (live today). May be a delay at TOD (propagation) | | | |
| 16 | DHCP | Yellow | 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 | Green | In production - no work necessary at TOD | | | |
| 18 | Internet | Green | Will be available | | | |
| Essential Infrastructure Services (Authentication/AD/File&Print/Apps/DB/Remote Access/Internet/Monitoring/MDM/Backup) | | | | | | |
| 19 | Authentication | Green | Domain Controller is currently active (1 VM + 1 Physical) | | | |
| 20 | Remote Access (VPN) | Green | | | | |
| 21 | SQL | Green | Requires Database team to recover (SRM) | | | |
| 22 | Oracle | Yellow | Requires Database team to recover (SRM) | | | |
| 23 | File/Print | Green | Need to test printing recovery | | | |
| IT Business Services (Helpdesk/VoIP/Email/GIS/Reporting/Project Management/Development Services) | | | | | | |
| 24 | Helpdesk | Green | TrackIT – fat client - DB is replicating (SQL) | | | |
| 25 | GIS | Yellow | Need recovery steps | | | |
| 26 | Email | Yellow | Will be moving to O365 first week of April | | | |

Town of Caledon Disaster Recovery Playbook – Administration Building Data Center

| Current State | | | | active | warning | issue |
|---------------|-----------------------|--------|---|--------|---------|-------|
| Item# | Description | Status | Notes | | | |
| 27 | VOIP (phone system) | green | Should failover but this needs to be tested | | | |
| 28 | External Websites (5) | red | Hosted by third-party + internal (not currently replicated) | | | |
| 29 | Reporting | red | | | | |

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

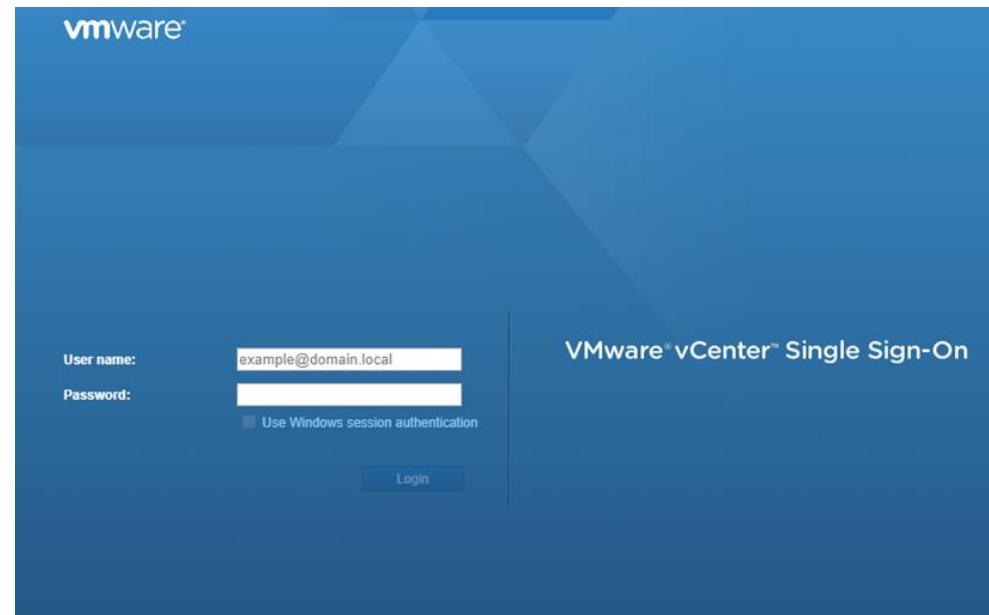
*Networking gear doesn't need to be shutdown

VMware Recovery Steps

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

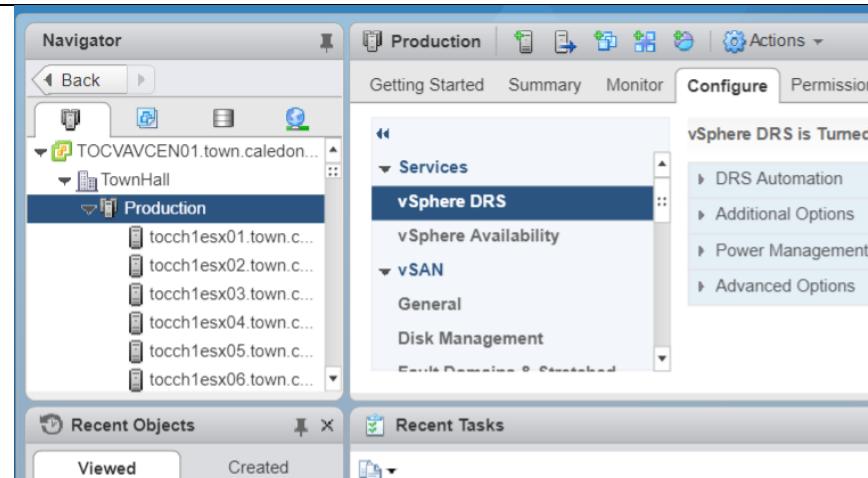
2. Click on vSphere Web Client (Flash)

3. Login with your Domain Admin account



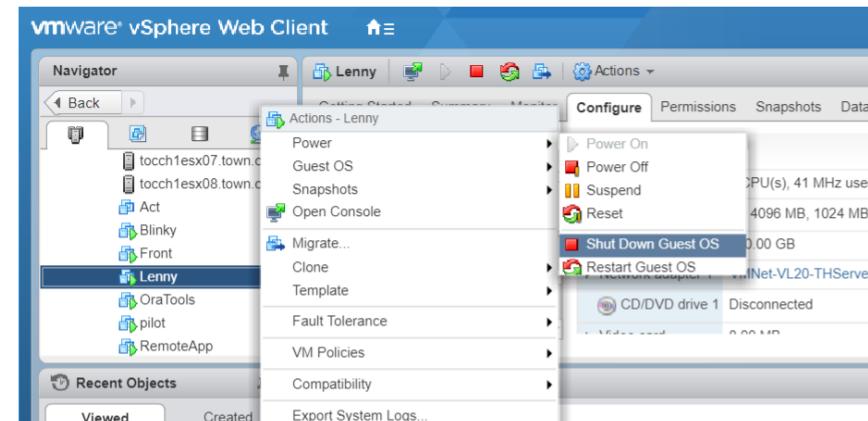
Primary Datacenter Shutdown Steps (continued)

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

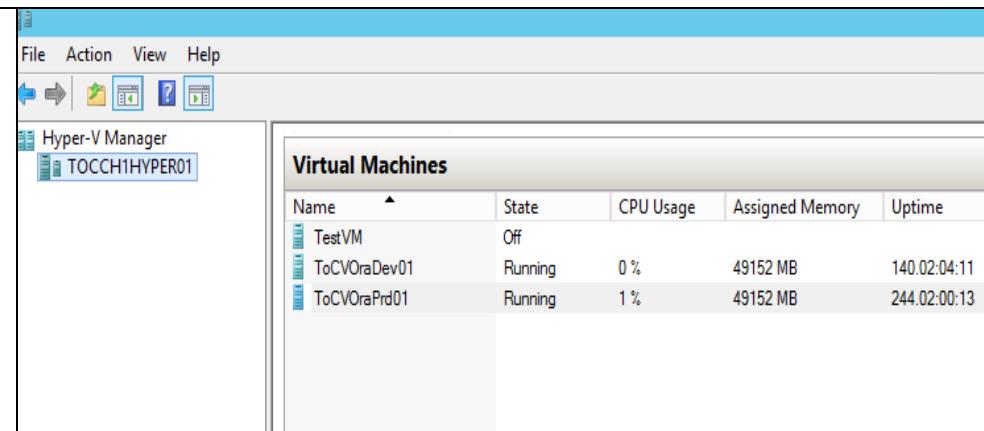
Important: Make a note of VMs that are already shutdown as they won't need to be powered on when bringing the VMs back online at the Primary DC.



Hyper-V Recovery Steps

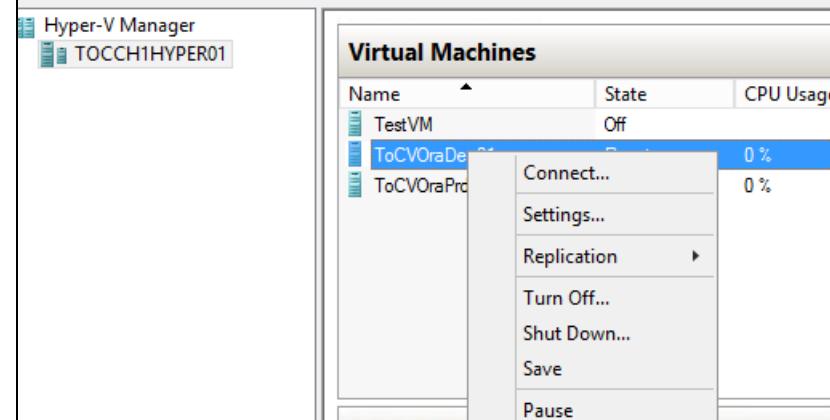
1. RDP to Hyper-V host - Server name: TOCCH1HYPER01

2. Launch "Hyper-V Manager"

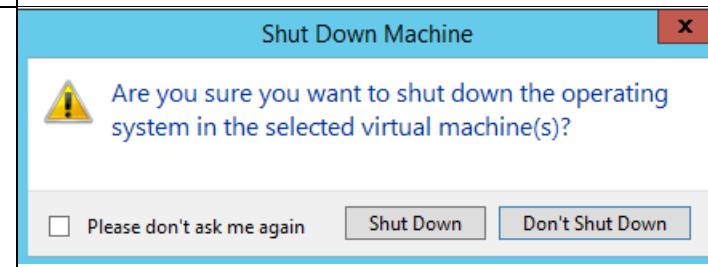


3. Right click the VM you wish to shutdown and click Shut Down.

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.



4. Click "Shutdown" again to confirm



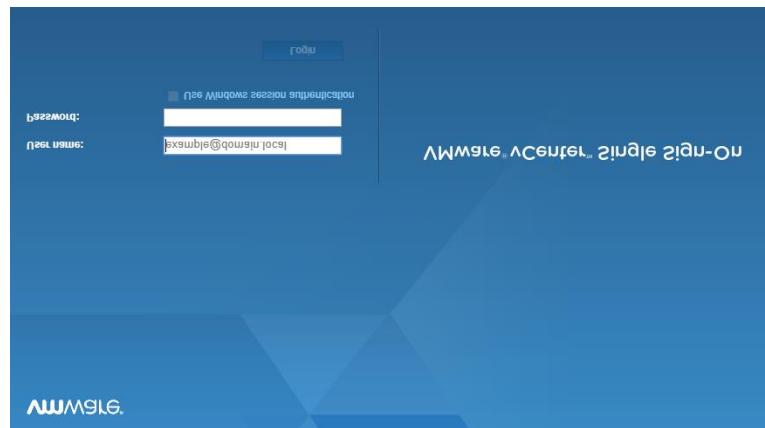
Chassis Nodes

VMware: The chassis nodes can be shutdown through vsphere web client used in the previous section to shutdown VMs

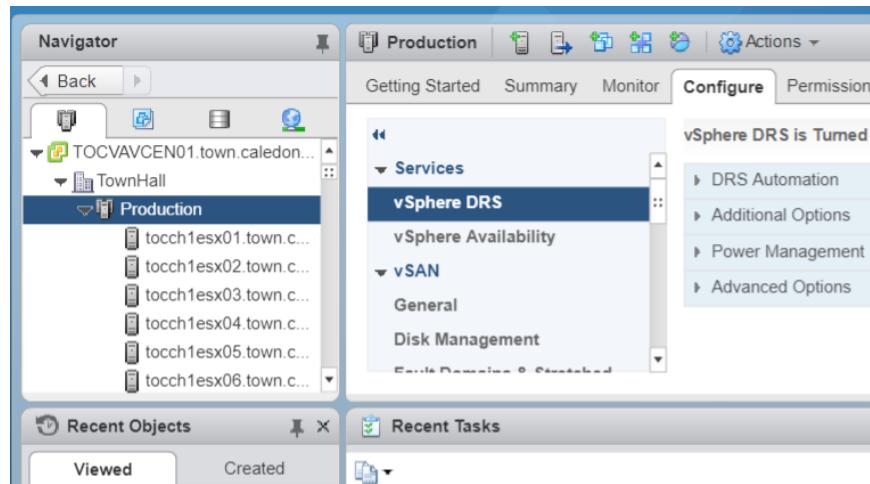
1. Open a web browser and browse to:<https://tocvavcen01>

2. Click on vSphere Web Client (Flash)

3. Login with your domain admin account

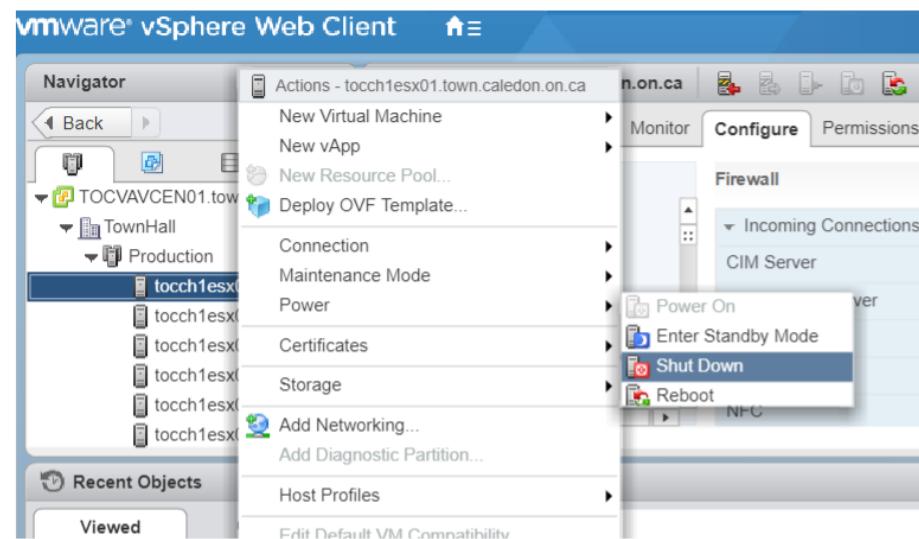


4. Expand the Production Cluster under Host & Clusters



5. Right click the Host and select Power then click "Shutdown"

Note: Ensure all VMs are shutdown on the Host



6. Repeat the previous step for all the Hosts.

Hyper-V

1. RDP to Hyper-v host - Server name: TOCCH1HYPER01

2. Click on Start and shutdown - **Ensure the VMs are powered off first

SAN

Follow the steps below to shutdown the Unity SAN at Town Hall.

Note: Complete shutdown and verification requires personnel on site.

1. Log into to Unisphere Prod (<https://unity-prod/>)

2. In Unisphere, select Service, under the System heading, then select Service Tasks.

3. Select Storage System > Shut Down Storage System, then Execute. Check the status of the shutdown process by looking at the SP LED indicators. The shutdown process is complete when the two power supply LEDs are solid green and amber, the network management port LEDs are flashing amber and green, and all other SP LEDs are off.

4. After confirming successful SP shutdown, remove all power from the SPs by disconnecting the two power cables from the Disk Processor Enclosures (DPE).

Wait 10 seconds and confirm that both the green and amber LEDs have turned off after the power cables are removed.

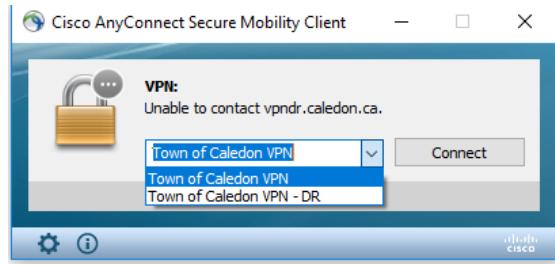
5. If you are relocating hardware, also disconnect the two power cables from each Disk Array Enclosure (DAE) to power them down.

Appendix D – VPN Access

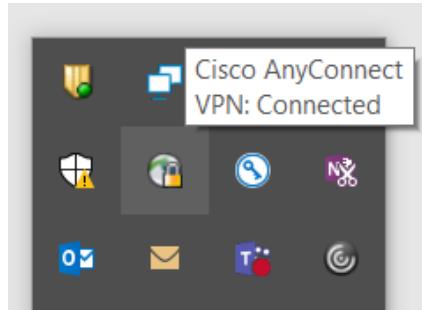
VPN Access Recovery Steps

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.



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.



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

Telephony (VOIP) Recovery

Steps to Failover

The following should failover automatically to DR site:

- The main phone number for Caledon (905-574-2272) should failover automatically to DR site.
- Phones at sites with connectivity to DR site should automatically connect to phone controller at DR site.

The following steps need to be done manually:

- Need to failover a VM named TOCVMAS01 (Voicemail/AutoAttendant) to the DR site through VMware SRM.
- For steps on SRM failover, refer to Annex X and use 'Mitel_Prod_ProtectionGroup' as the group being failed over.

Testing

Once the telephone system has been failed over as indicated in the previous section. Test the following to confirm availability of services:

- Ensure a successful call to an external number (from a site with connectivity to DR site e.g. CCRW)
- From a mobile phone call the Town of Caledon main line (905-574-2272) and confirm the Auto Attendant answers and you are able to reach an extension (at sites with connectivity to DR site e.g CCRW)

Troubleshooting: Confirm Core Infrastructure and Physical Infrastructure services are available. Refer to Appendix L and M.

Appendix F – Email Testing

Email Recovery

Steps to Failover

- The email system is provided through O365.
- Mailboxes reside in O365 and mail routing is done through O365.
- Users simply need an internet connection in order to access email.

Exception:

The only exception to this is systems that rely on internal mail relay e.g. If an application sends an email internally or externally, it would connect to the on-premise exchange server. The exchange server (Blinky) will need to be failed over through SRM.

Refer to Appendix H and use 'Prod_ProtectionGroup' as the group being failed over.

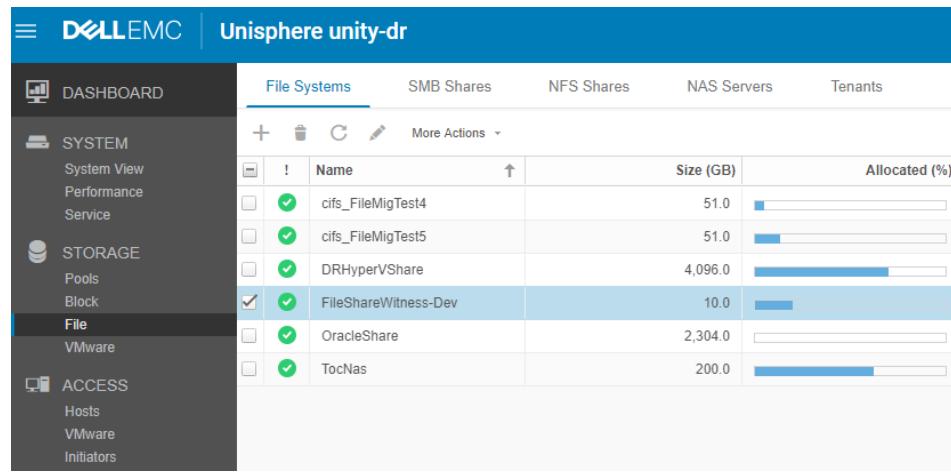
Important: Don't failover 'Prod_ProtectionGroup' until you have completed Step X (Database Recovery) in the restoration table. Initiating the failover will power on the VMs at the DR site which would require the Databases to be available first, in order for the application to function.

Testing

- Confirm Outlook can connect to exchange on a machine located at DR site or at a site with connectivity to DR site.

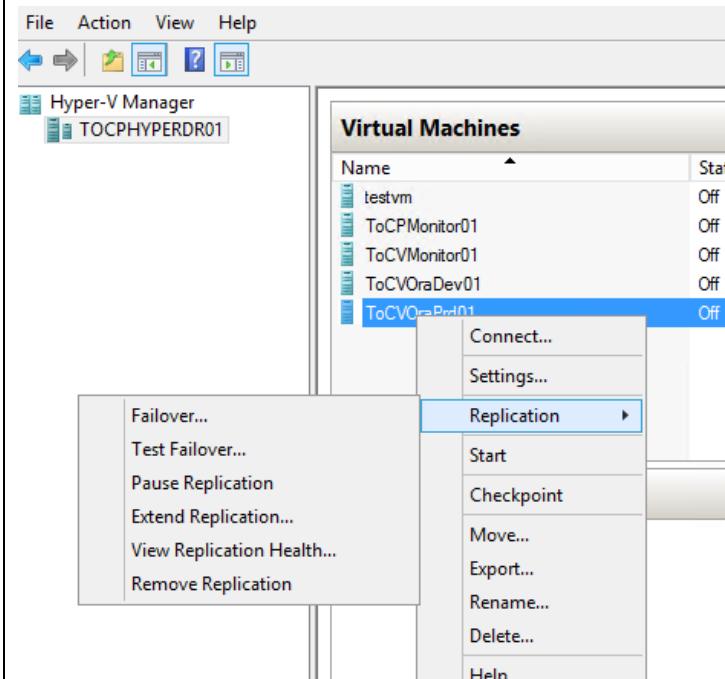
Troubleshooting: Confirm Core Infrastructure and Physical Infrastructure services are available. Refer to Appendix L and M.

Appendix G – Database Recovery

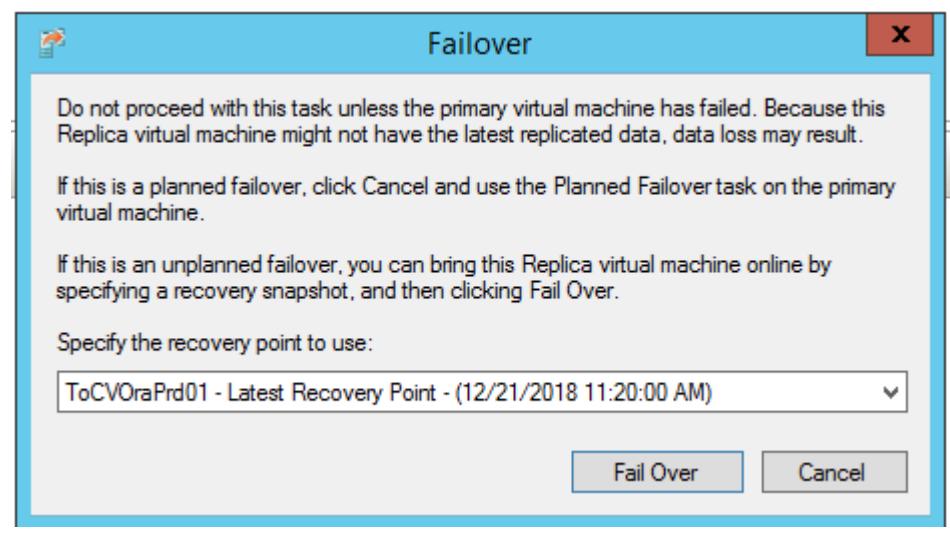
| Database Recovery | | | | | | | | | | | | | | | | | | | | | | |
|--|--|---------------|-----------|---------------|-------------------|------|-----|-------------------|------|-----|---------------|---------|-----|-----------------------------|------|-----|-------------|---------|-----|--------|-------|-----|
| SQL Database | | | | | | | | | | | | | | | | | | | | | | |
| <p>The SQL servers are setup in a Geo-Cluster which requires manual intervention in order to failover to the DR site. The following procedures apply if the SQL database servers at TH site are shutdown or not reachable through the network.</p> | | | | | | | | | | | | | | | | | | | | | | |
| <p>1. Log into the Unity-DR to move over the Fileshare Witness: Log into https://10.10.8.100</p> | | | | | | | | | | | | | | | | | | | | | | |
| <p>2. From the left menu click on File under the Storage heading</p> | | | | | | | | | | | | | | | | | | | | | | |
| 3. Select the FileShareWitness-Prod File System and click the edit icon. |  <table border="1"><thead><tr><th>Name</th><th>Size (GB)</th><th>Allocated (%)</th></tr></thead><tbody><tr><td>cifs_FileMigTest4</td><td>51.0</td><td>10%</td></tr><tr><td>cifs_FileMigTest5</td><td>51.0</td><td>10%</td></tr><tr><td>DRHyperVShare</td><td>4,096.0</td><td>90%</td></tr><tr><td>FileShareWitness-Dev</td><td>10.0</td><td>10%</td></tr><tr><td>OracleShare</td><td>2,304.0</td><td>10%</td></tr><tr><td>TocNas</td><td>200.0</td><td>10%</td></tr></tbody></table> | Name | Size (GB) | Allocated (%) | cifs_FileMigTest4 | 51.0 | 10% | cifs_FileMigTest5 | 51.0 | 10% | DRHyperVShare | 4,096.0 | 90% | FileShareWitness-Dev | 10.0 | 10% | OracleShare | 2,304.0 | 10% | TocNas | 200.0 | 10% |
| Name | Size (GB) | Allocated (%) | | | | | | | | | | | | | | | | | | | | |
| cifs_FileMigTest4 | 51.0 | 10% | | | | | | | | | | | | | | | | | | | | |
| cifs_FileMigTest5 | 51.0 | 10% | | | | | | | | | | | | | | | | | | | | |
| DRHyperVShare | 4,096.0 | 90% | | | | | | | | | | | | | | | | | | | | |
| FileShareWitness-Dev | 10.0 | 10% | | | | | | | | | | | | | | | | | | | | |
| OracleShare | 2,304.0 | 10% | | | | | | | | | | | | | | | | | | | | |
| TocNas | 200.0 | 10% | | | | | | | | | | | | | | | | | | | | |

| | |
|--|---|
| <p>4. Click on the Replication tab and click Failover to initiate the process.</p> | |
| <p>5. The SQL instances should now be UP at DR site</p> | <p>Connect to the appropriate SQL server at the DR and launch Failover Cluster Manager to confirm.</p> <p>Currently, the following production servers exist at DR site:</p> <ul style="list-style-type: none"> • TOCVSQLDR31 • TOCVSQLDR32 • TOCSQLDR22 • TOCVSQLDR21 |
| <h2>Oracle Database Recovery</h2> | |
| <p>Oracle databases servers run in a clustered Hyper-V environment, with a host at each site (Towhall and DR site). In a DR scenario, we will connect to the DR site host and initiate failover of the VM.</p> | |
| <p>1. RDP to the Hyper-V host at DR site - Hostname: TOCPHYPERDR01 IP: 10.2.23.14</p> | |
| <p>2. Launch Hyper-V Manager - Click start and type 'Hyper-V Manager'</p> | |
| <p>3. Right click on 'ToCVOraPrd01'</p> | |

4. Click on Failover under Replication.



5. Select the Latest Recovery Point and click **Fail Over**.



Appendix H – File Services Recovery

Currently the FileShares are hosted on 2 different platforms:

| Share Name/Drive | Platform | Notes |
|------------------|-----------------------------|----------------------------|
| U drive | VNX SAN | |
| K drive | Windows File Server Cluster | \File and \File-Inf shares |
| S drive | VNX SAN | |
| W drive | VNX SAN | |
| N drive | VNX SAN | |
| V drive | VNX SAN | |

Steps to Failover Windows File Server Cluster (\File and \File-Inf shares)

| | |
|--|--|
| 1. Ensure the cluster witness share has already been failed over. | Ensure that steps 1 – 4 for SQL Database Recovery listed in Annex C have already been completed and the 'FileShareWitness-Prod' has already been failed over to DR site. |
| 2. RDP to TOCVFILEDR01 and launch Failover Cluster Manager | |
| 3. Click on the Cluster object and confirm the File Share Witness is visible | INSERT SCREENSHOT |

4. Expand the cluster object and click on Roles

The screenshot shows the Failover Cluster Manager interface. On the left, there's a navigation pane with 'File', 'Action', 'View', and 'Help' menus, and icons for 'Cluster', 'File', 'Network', and 'Event'. Below that is a tree view under 'Failover Cluster Manager' for 'FileCL01.town.caledon.on.ca': 'Nodes', 'Storage', 'Networks', and 'Cluster Events'. The main area is titled 'Roles (2)' with a search bar. It contains a table with columns: Name, Status, Type, Owner Node, Priority, and Information. There are two entries: 'Files' (Running, File Server, ToCVFile01, Medium) and 'Files-Inf' (Running, File Server, ToCVFile02, High).

5. Confirm the 'Files' and 'Files-inf' roles are running on TOCVFILEDR01 and TOCVFILEDR02

6. Confirm the file share(s) can be accessed through Windows Explorer

The screenshot displays two separate instances of Windows Explorer. The top instance is titled 'files' and shows a folder structure on the left with 'Quick access', 'Desktop', 'Documents', 'Downloads', and 'Pictures'. On the right, there are two network shares: 'Caledon' (yellow icon) and 'Test' (yellow icon). The bottom instance is titled 'files-inf' and also shows a similar folder structure on the left. On the right, it shows three network shares: 'GIS' (yellow icon), 'RDS' (yellow icon), and 'SCCM' (yellow icon).

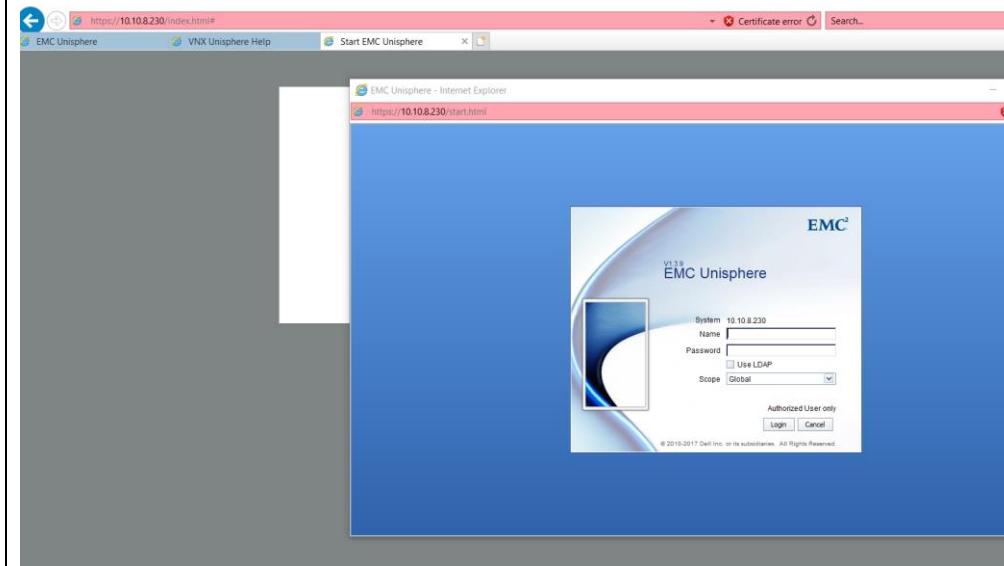
Steps to Failover File Shares on EMC VNX (Coltrane)

1. Connect to EMC VNX SAN at DR site - <https://10.10.8.230>

Note: The web application requires Java. You will likely need to add the IP address to trusted sites under Java Exception site list (from the control panel). Additionally, there are several security related pop-ups and warnings that must be accepted to get to the login screen.

2. Enter the credentials

Note: Credentials can be found in PasswordState



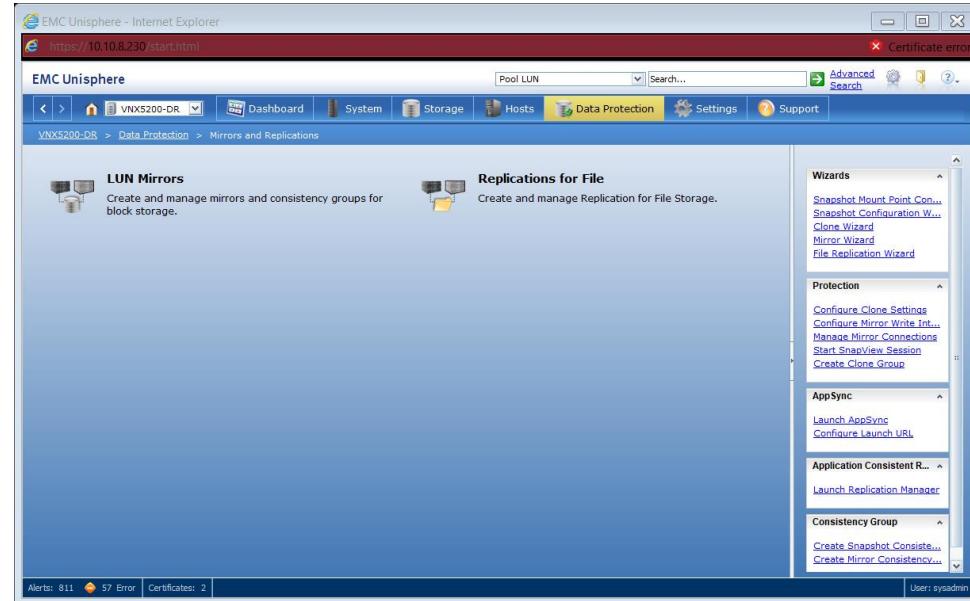
3. Select VNX5200-DR from the drop down menu.

The screenshot shows the EMC Unisphere interface for the VNX5200-DR system. On the left, a sidebar lists 'System Alerts (10 of 406)' with severity, created date, message, and event code. On the right, the 'System Information' panel displays the system's status as 'Error (27)', name 'VNX5200-DR', model 'VNX5200 (Unified)', and various IP addresses and serial numbers. Below it, the 'Storage Capacity Summary' section features a pie chart illustrating disk usage: Used (33807.19 GB), Free Raw Disk (2371.1 GB), Free Storage Pool (27308.37 GB), and Free Space for File (65.12 GB).

4. Click on Data Protection and then Mirrors and Replications

The screenshot shows the 'Data Protection' section of the EMC Unisphere interface. It includes four main sections: 'Snapshots' (Create and manage LUN Snapshots and File System Checkpoints), 'Clones' (Create and manage clones for block storage), 'Mirrors and Replications' (Create and manage Mirrors and consistency groups for Block Storage, and Replication for File Storage), and 'Reserved LUN Pool' (View details of the storage systems Reserved LUN Pool). A vertical 'Wizards' column on the right provides links for Snapshot Mount Point Configuration, Snapshot Configuration Wizard, Clone Wizard, Mirror Wizard, and File Replication Wizard. Other sections like 'Protection', 'AppSync', 'Application Consistent R...', and 'Consistency Group' also have their own sub-links.

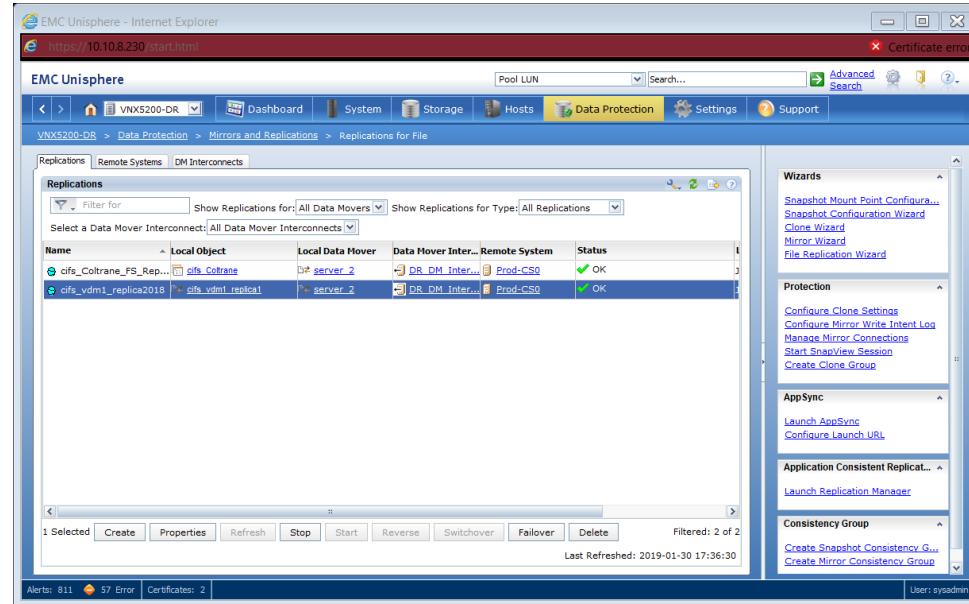
5. Click on Replications for File



6. First select **cifs_dm1_replica2018** and then click on **Failover**

Note: Once the data mover is failed-over we can move the file system as follows:

Select **cifs_Coltrane_FS_Replication** and then click **Failover**



7. Once failed over DNS might need a manual update:

Go to TOCVDCDR01 and Open DNS and see if Corane now points to “10.10.9.232”. If not modify the A record for Coltrane as needed.

Note: The TTL for Coltrane is set to 20 mins so it could take up to 20 mins before clients will get the updated DNS record.

Appendix I – Print Services Recovery

Printing Services Recovery

There are **3** main components to printing at Town of Caledon.

1. Printer server
2. Equitrac Cluster (Follow-you-Printing)

Note: Servers related to both of these components need to be failed over in order for follow-you printing to work.

Print Server failover:

- The print server (TOCPRT01) is failed over and powered on as part of VMware SRM (Annex X) which was done previously.
- Confirm you can connect to TOCVPRINT01 and it appears to be in a healthy state.

Equitrac Cluster failover:

Note: The steps below are not complete due to the nature of the failover. Please review all the steps below and devise a plan of action for the missing steps before proceeding.

1. Log into the Unity SAN at DR site.
2. From the left menu click on Block under Storage

| | Name | Size |
|--------------------------|-----------------------|------|
| <input type="checkbox"/> | DRDevSQLCL03-EXT-Data | |
| <input type="checkbox"/> | DRDevSQLCL03-EXT-Log | |
| <input type="checkbox"/> | DRDevSQLCL03-EXT-Rep | |

3. From tabs at the top Select Consistency Groups and then ToCVEquiCL01

The screenshot shows the Dell EMC Unisphere unity-dr interface. The left sidebar has categories: DASHBOARD, SYSTEM, STORAGE, and ACCESS. Under STORAGE, the 'Block' option is selected. The main area has tabs: LUNs, Consistency Groups (which is selected), and iSCSI Interfaces. Below the tabs is a table of LUNs:

| | Name | Size (GB) | Allocated (%) |
|-------------------------------------|--------------|-----------|----------------|
| <input type="checkbox"/> | DRDevSQLCL03 | 369.5 | [Progress Bar] |
| <input type="checkbox"/> | DRDevSQLCL04 | 766.0 | [Progress Bar] |
| <input type="checkbox"/> | DRFileCL01 | 8,212.0 | [Progress Bar] |
| <input type="checkbox"/> | DRSQLCL03 | 584.5 | [Progress Bar] |
| <input type="checkbox"/> | DRSQLCL04 | 1,167.5 | [Progress Bar] |
| <input checked="" type="checkbox"/> | ToCVEquiCL01 | 12.0 | [Progress Bar] |

Below the table, a modal window titled 'ToCVEquiCL01 Properties' is open. It has tabs: General, LUNs, Host Access, Snapshots, and Replication (which is selected). The 'Replication' tab displays the following details:

- Session Name: rep_sess_res_28_res_27_APM00173126802_APM00173126807
- Mode: Asynchronous, 60 minutes
- Local Role: Destination
- Time of Last Sync: 1/30/2019, 3:29:53 PM
- Replicate Scheduled Snapshots: No

Below these details is a diagram illustrating the replication flow. It shows an 'I/O' arrow pointing down to a stack of three cylinders labeled 'APM00173126802 (10.2.20.100) ToCVEquiCL01'. An arrow points from this stack to another stack of three cylinders labeled 'Local System ToCVEquiCL01'. Between the two stacks is a green circle with a checkmark and the text 'Auto Sync Configured'. At the bottom of the replication section are several buttons: Delete, Pause, Resume, Sync, Failover (which is highlighted in blue), Failover with sync, and Fallback.

4. Click the Edit icon to open the Properties. Then click on the Replication tab.

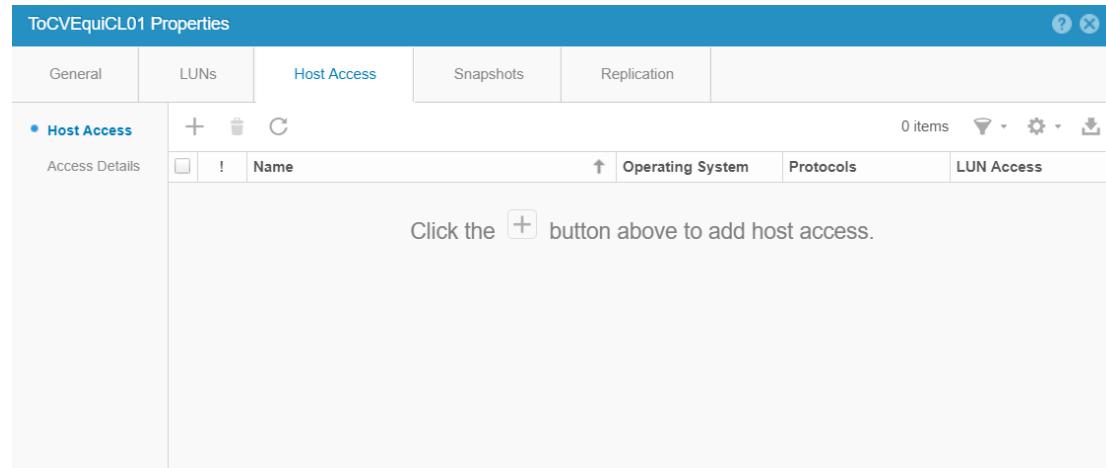
5. Click on Failover to initiate failover of the disks.

6. Ensure both servers in the Equitrac are failed over

Note: Following the steps to manually failover VMware VMs (as indicated in Appendix X), make sure you failover and power on TOCQEQUI01 and TOCQEQUI02

7. Return to the DR SAN web console and add host access to the storage

Note: Add TOCEQUI01 and TOCEQUI02 under Host Access of ToCVEQUICL01 storage



8. Final steps not determined.

At a high level the following would need to be accomplished:

1. Connect both server Equi01 and Equi02 to the storage using isci initiator configuration
2. Ensure the storage is visible under the cluster
3. Ensure the Disk Witness is visible
4. Once the Windows Cluster is healthy, attempt to start the application (Equitrac).

Appendix J – Helpdesk Recovery

Appendix K – GIS Recovery

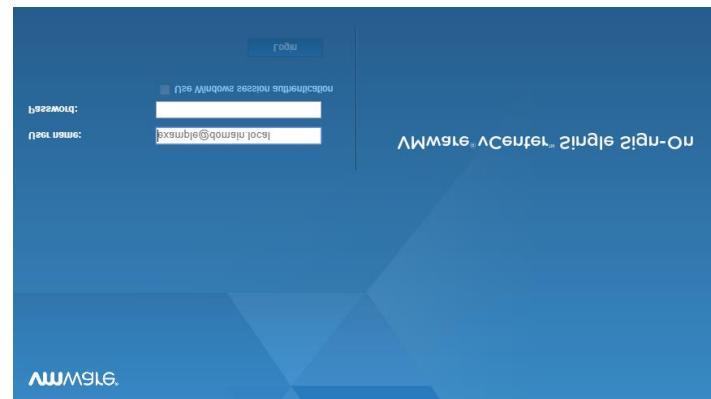
Appendix L – Software Defined Infrastructure Recovery

VMware (SRM) Failover

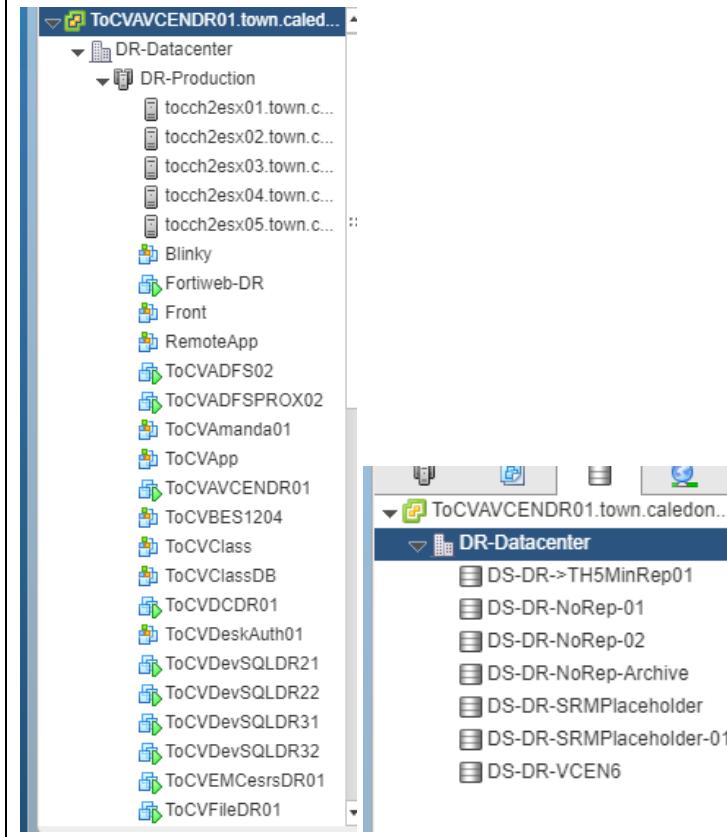
1. Open a web browser and browse to: <https://tovcavcendr01>

2. Click on vSphere Web Client (Flash)

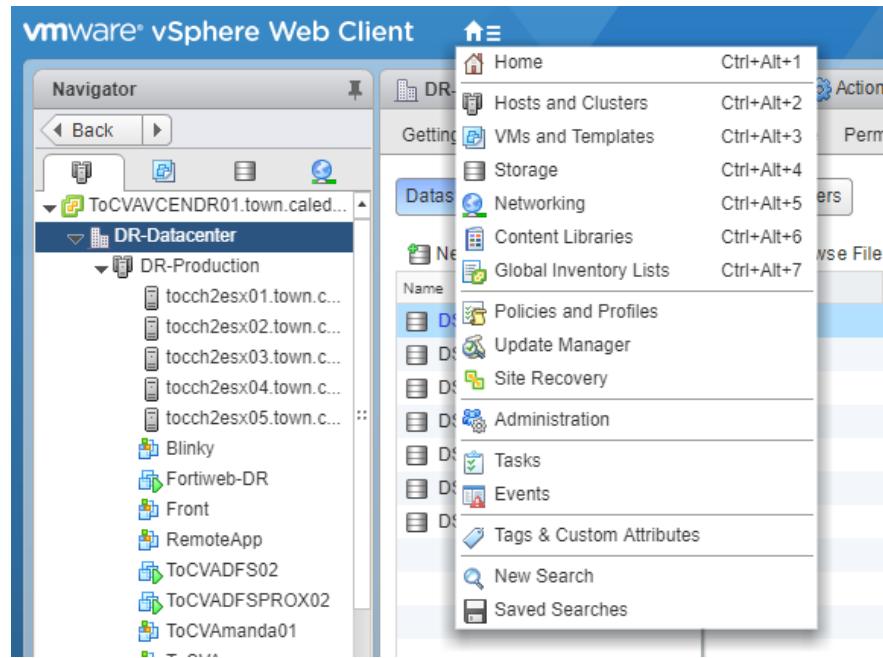
3. Login with your Domain Admin account



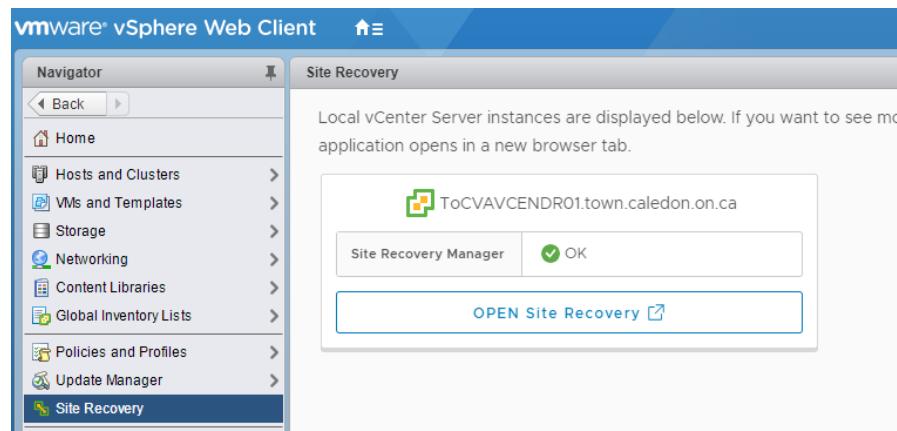
4. After a successful login, confirm the hosts and storage are connected to the DR site VMware environment and there are no Alarms or errors.



5. From the top left – click on the Home icon and select Site Recovery.



6. Click on “Open Site Recovery”. This will launch a new browser window.



7. Once the Site Recovery window opens. Click on "View Details"

The screenshot shows a web browser window with the URL <https://10.10.20.15/dr/#/home>. The page title is "Site Recovery". A "NEW SITE PAIR" button is visible. Below it, a site pair is listed: "ToCVAVCENDR01.town.caledon.on.ca" and "TOCVAVCEN01.town.caledon.on.ca" with a double-headed arrow between them. The interface includes sections for "Site Recovery Manager", "Protection Groups 2", and "Recovery Plans 2". At the bottom are "VIEW DETAILS" and "ACTIONS" buttons.

8. Enter your login information. Make sure to prefix with domain name. (Domain admin credentials)

The dialog box is titled "Log In Site". It contains fields for "vCenter Server" (set to TOCVAVCEN01.town.caledon.on.ca), "User name" (with placeholder "Enter user name"), and "Password" (with placeholder "Enter password"). At the bottom are "CANCEL" and "LOG IN" buttons.

9. Click on “Protection Groups”. Then click on “Mitel_Prod_ProtectionGroup”.

| Name | Protection Status |
|----------------------------|-------------------|
| Mitel_Prod_ProtectionGroup | OK |
| Prod_ProtectionGroup | OK |

10. Click on the Virtual Machines tab to review the list of VMs that will be recovered.

| Virtual Machine | Protection Status |
|-----------------|-------------------|
| ToCVMAS01 | OK |

11. Click on the Recovery Plans tab and Select the associated recovery plan.

| Name | Status |
|-------------------------|--------|
| Mitel_Prod_RecoveryPlan | Ready |
| Prod_RecoveryPlan | Ready |

12. Click Run to initiate the recovery.

The screenshot shows the 'Recovery Plans' section of a software interface. At the top, there are tabs for 'Site Pair', 'Protection Groups', and 'Recovery Plans'. Below the tabs is a search bar labeled 'Search...'. A list of 'Recovery Plans' is displayed, with two items shown: 'Mitel_Prod_RecoveryPlan' and 'Prod_RecoveryPlan'. Both items have a green circular icon with a play symbol next to them, indicating they are ready. To the right of the list is a toolbar with buttons for '+ NEW', 'EDIT', 'MOVE', 'DELETE', 'TEST', 'CLEANUP', 'RUN', and three dots. Below the toolbar is a table with columns 'Name' and 'Status'. The first row shows 'Mitel_Prod_RecoveryPlan' with a status of 'Ready'. The second row shows 'Prod_RecoveryPlan' with a status of 'Ready'.

13. The previous step will initiate recovery and the screen will display the steps and their progress.

The screenshot shows the 'Recovery Steps' interface for the 'Mitel_Prod_RecoveryPlan'. At the top, there are tabs for 'Summary', 'Recovery Steps', 'Issues', 'History', 'Permissions', 'Protection Groups', and 'Virtual Machines'. Below the tabs is a toolbar with buttons for 'EXPORT STEPS', 'TEST', 'CLEANUP', 'RUN', 'REPROTECT', and 'CANCEL'. The main area is divided into two sections: 'Plan status:' (Ready) and 'Description:' (This plan is ready for test or recovery). Below these is a table titled 'Recovery Step' with a column for 'Status'. The table lists ten steps, each preceded by a small colored icon and a number: 1. Synchronize storage (blue), 2. Restore recovery site hosts from standby (green), 3. Suspend non-critical VMs at recovery site (yellow), 4. Create writable storage snapshot (orange), 5. Configure test networks (purple), 6. Power on priority 1 VMs (red), 7. Power on priority 2 VMs (dark blue), 8. Power on priority 3 VMs (light blue), 9. Power on priority 4 VMs (teal), and 10. Power on priority 5 VMs (light purple).

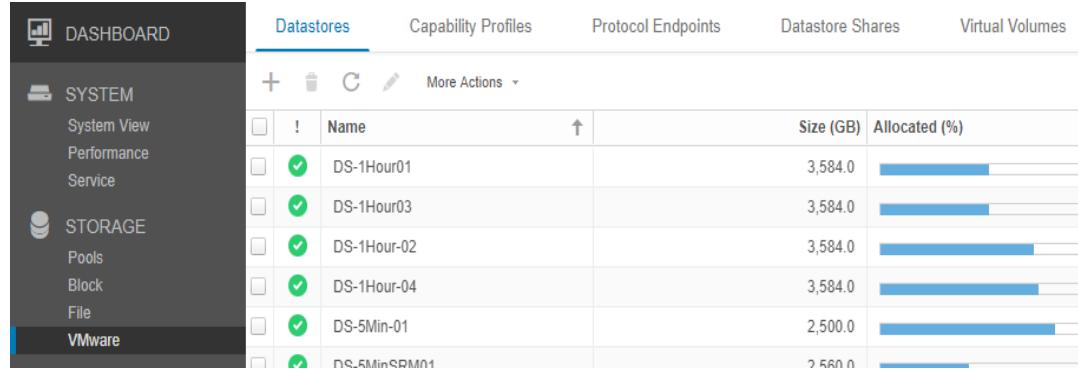
14. Repeat steps 9 to 12 for the other Protection group -“Prod_ProtectionGroup”

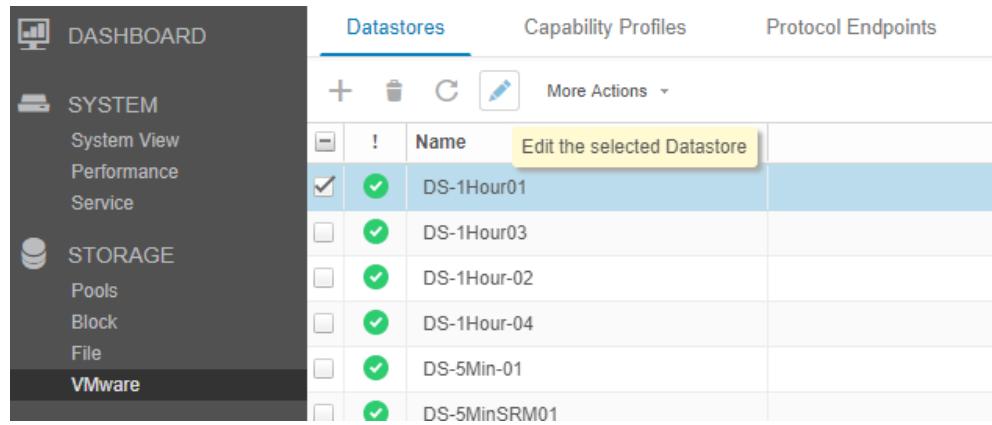
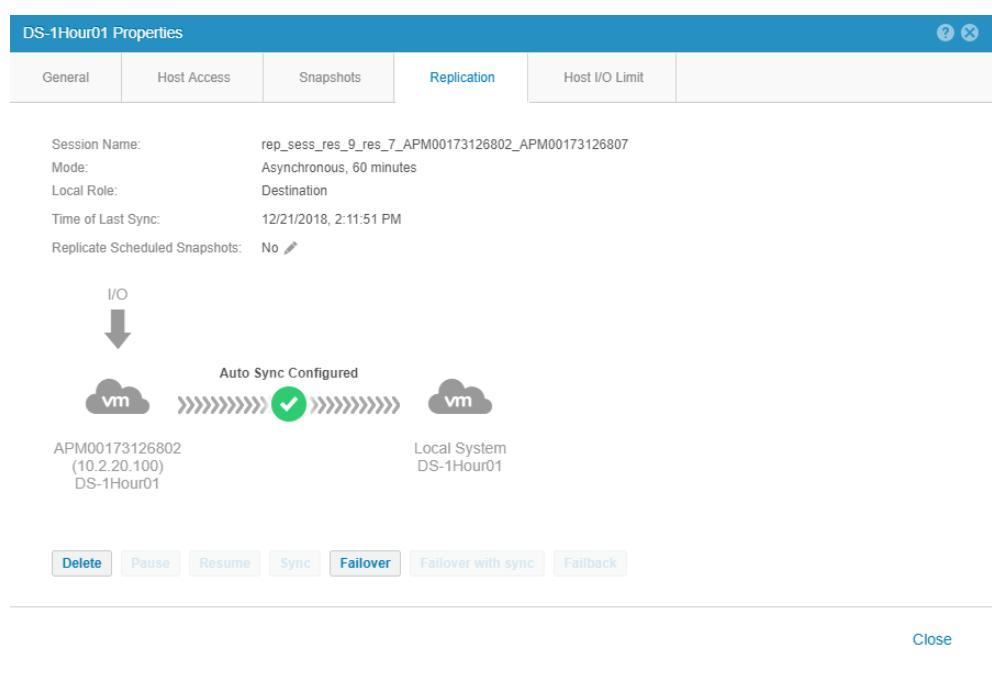
Important: Don't failover 'Prod_ProtectionGroup' until you have completed Step X (Database Recovery) in the restoration table. Initiating the failover will power on the VMs at the DR site which would require the Databases to be available first, in order for the application to function.

VMware (non-SRM) Failover

Up to 25 VMs can be automatically failed over using SRM. Any additional VMs that need to be failed over must be moved over manually. In order to qualify for manual failover, the VM must be stored on one of the following datastores (the naming convention is based on the recovery point the datastore offers).

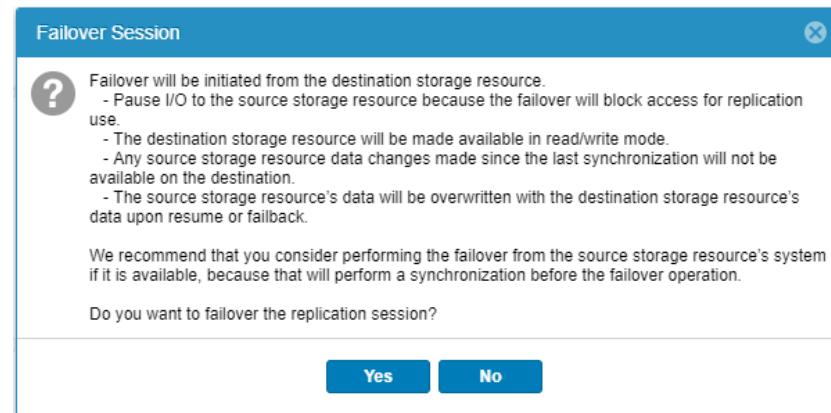
- DS-1Hour-01
- DS-1Hour-02
- DS-1Hour-03
- DS-1Hour-04
- DS-5Min-01

| 1. Log into the Unity SAN at DR site. | https://10.10.8.100 | | | | | | | | | | | | | | | | | | | | | |
|---|--|---------------|-----------|---------------|-------------|---------|------|-------------|---------|------|-------------|---------|------|-------------|---------|------|------------|---------|------|--------------|---------|------|
| 2. From the left menu click on VMware under Storage |  <table border="1"><thead><tr><th>Name</th><th>Size (GB)</th><th>Allocated (%)</th></tr></thead><tbody><tr><td>DS-1Hour-01</td><td>3,584.0</td><td>~80%</td></tr><tr><td>DS-1Hour-03</td><td>3,584.0</td><td>~80%</td></tr><tr><td>DS-1Hour-02</td><td>3,584.0</td><td>~80%</td></tr><tr><td>DS-1Hour-04</td><td>3,584.0</td><td>~80%</td></tr><tr><td>DS-5Min-01</td><td>2,500.0</td><td>~80%</td></tr><tr><td>DS-5MinSRM01</td><td>2,560.0</td><td>~80%</td></tr></tbody></table> | Name | Size (GB) | Allocated (%) | DS-1Hour-01 | 3,584.0 | ~80% | DS-1Hour-03 | 3,584.0 | ~80% | DS-1Hour-02 | 3,584.0 | ~80% | DS-1Hour-04 | 3,584.0 | ~80% | DS-5Min-01 | 2,500.0 | ~80% | DS-5MinSRM01 | 2,560.0 | ~80% |
| Name | Size (GB) | Allocated (%) | | | | | | | | | | | | | | | | | | | | |
| DS-1Hour-01 | 3,584.0 | ~80% | | | | | | | | | | | | | | | | | | | | |
| DS-1Hour-03 | 3,584.0 | ~80% | | | | | | | | | | | | | | | | | | | | |
| DS-1Hour-02 | 3,584.0 | ~80% | | | | | | | | | | | | | | | | | | | | |
| DS-1Hour-04 | 3,584.0 | ~80% | | | | | | | | | | | | | | | | | | | | |
| DS-5Min-01 | 2,500.0 | ~80% | | | | | | | | | | | | | | | | | | | | |
| DS-5MinSRM01 | 2,560.0 | ~80% | | | | | | | | | | | | | | | | | | | | |

| | |
|---|---|
| <p>3. Select Datastore that needs to be failed over and click the edit icon.</p> <p>e.g. DS-1Hour01</p> |  |
| <p>4. Click on the Replication tab and then Failover</p> |  |

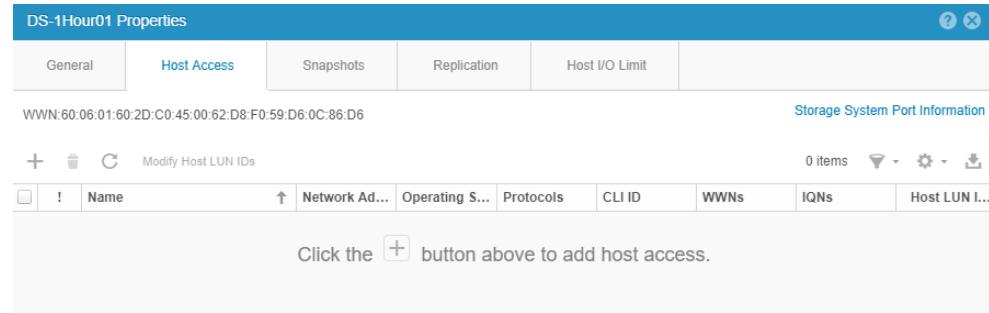
5. Confirm the source datastore is no longer being used. Then Click Yes

Note: This may involve manually shutting down the VMs at the source datastore (Depending on the nature of the DR scenario)

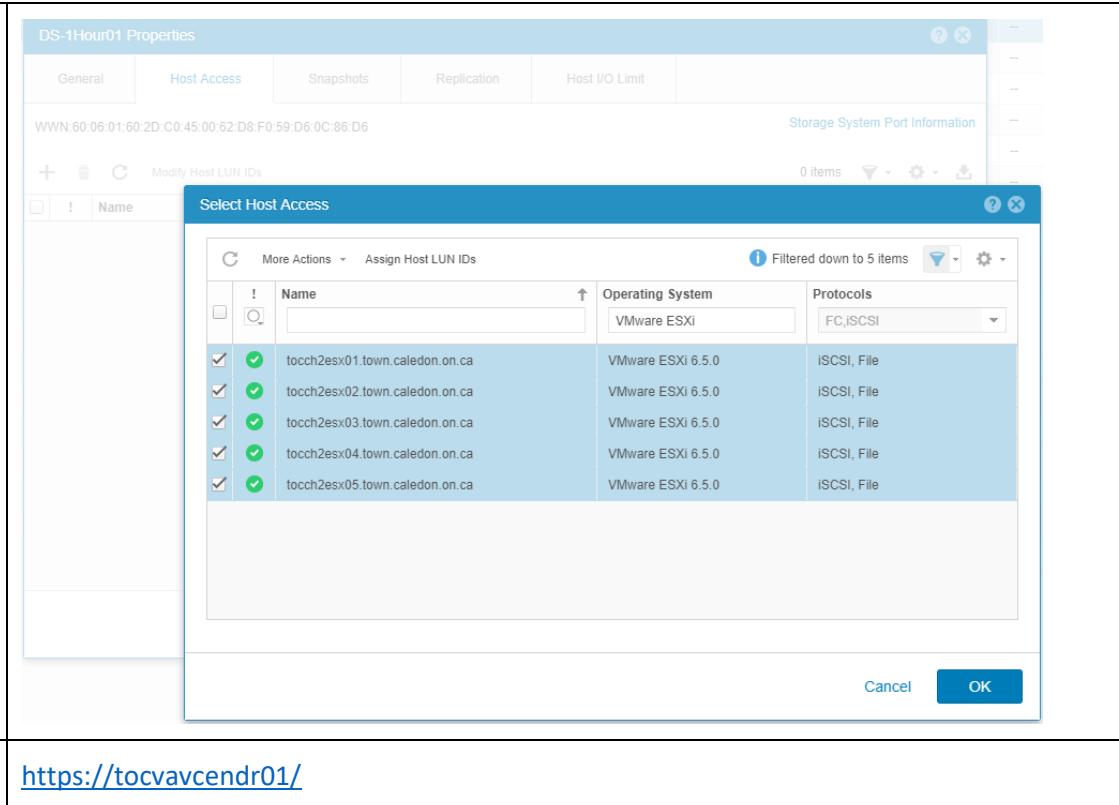


6. Once the datastore is failed over – provide the DR hosts access to the Datastore

Note: Under the datastore properties click on Host Access



7. Click the + sign to add access. Select all the hosts and click OK.



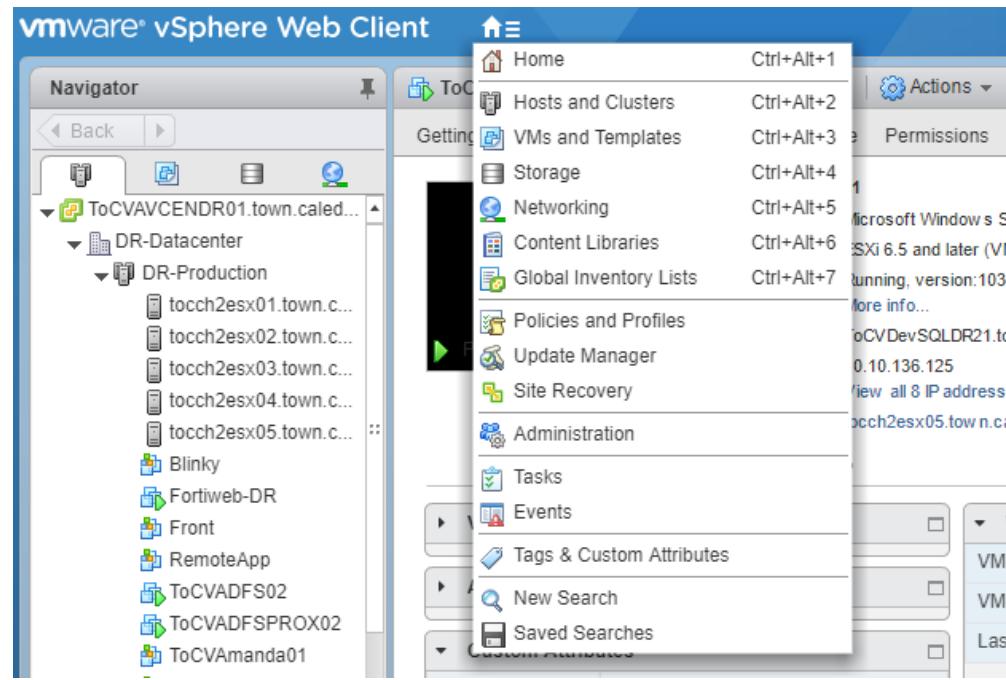
The screenshot shows the 'DS-1Hour01 Properties' window with the 'Host Access' tab selected. Below it is the 'Select Host Access' dialog box. The dialog has a header with 'Assign Host LUN IDs' and a note 'Filtered down to 5 items'. It contains a table with columns: Name, Operating System, and Protocols. Five hosts are listed, all with checkboxes checked and green checkmarks. The hosts are: tocch2esx01.town.caledon.on.ca, tocch2esx02.town.caledon.on.ca, tocch2esx03.town.caledon.on.ca, tocch2esx04.town.caledon.on.ca, and tocch2esx05.town.caledon.on.ca. All hosts are running VMware ESXi 6.5.0 and are assigned to iSCSI, File protocols. At the bottom right of the dialog are 'Cancel' and 'OK' buttons.

| Name | Operating System | Protocols |
|--------------------------------|-------------------|-------------|
| tocch2esx01.town.caledon.on.ca | VMware ESXi 6.5.0 | iSCSI, File |
| tocch2esx02.town.caledon.on.ca | VMware ESXi 6.5.0 | iSCSI, File |
| tocch2esx03.town.caledon.on.ca | VMware ESXi 6.5.0 | iSCSI, File |
| tocch2esx04.town.caledon.on.ca | VMware ESXi 6.5.0 | iSCSI, File |
| tocch2esx05.town.caledon.on.ca | VMware ESXi 6.5.0 | iSCSI, File |

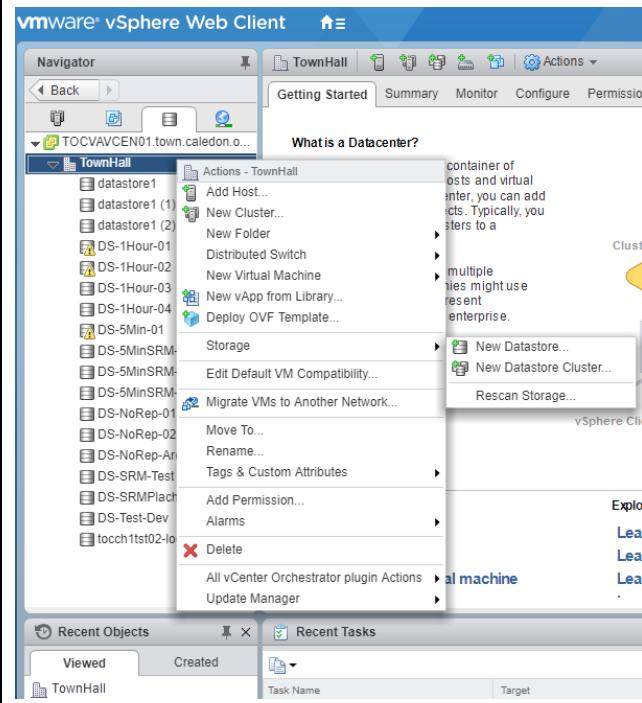
8. Log into vCenter at DR site

<https://tocvavcendr01/>

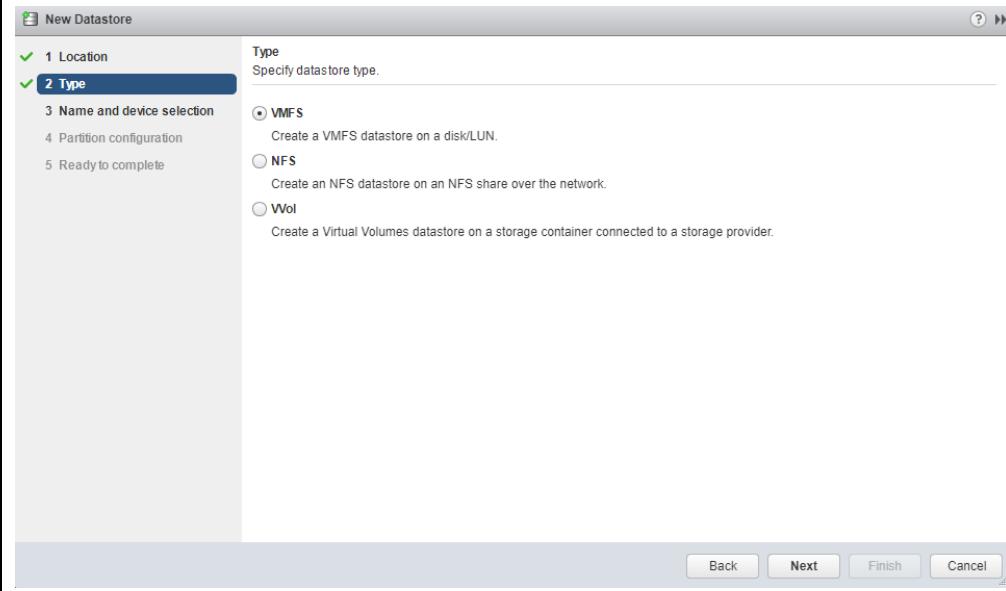
9. From the top menu select Storage.



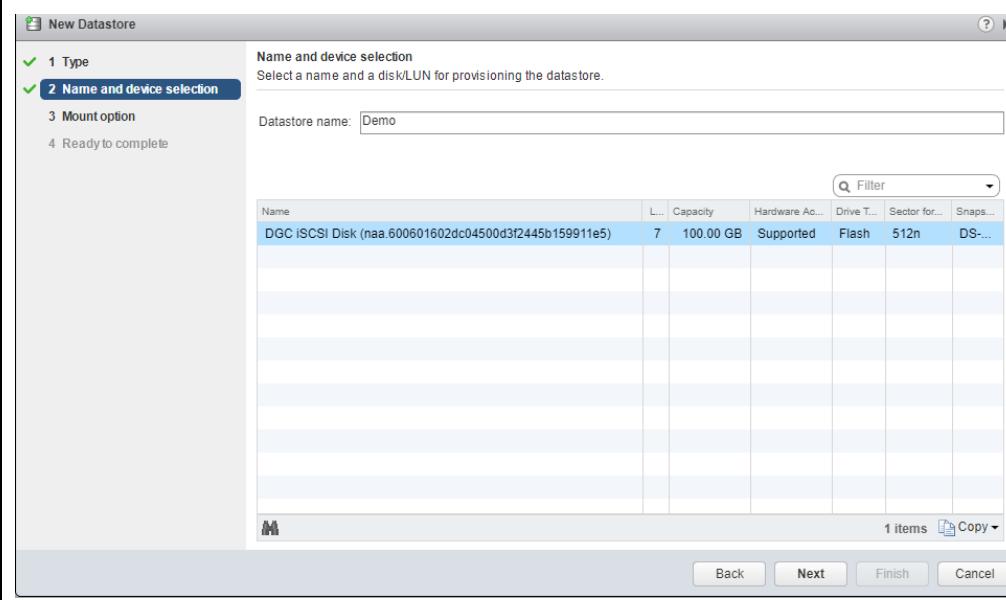
10. Right click ‘TownHall’ and select ‘New Datastore’ under Storage.



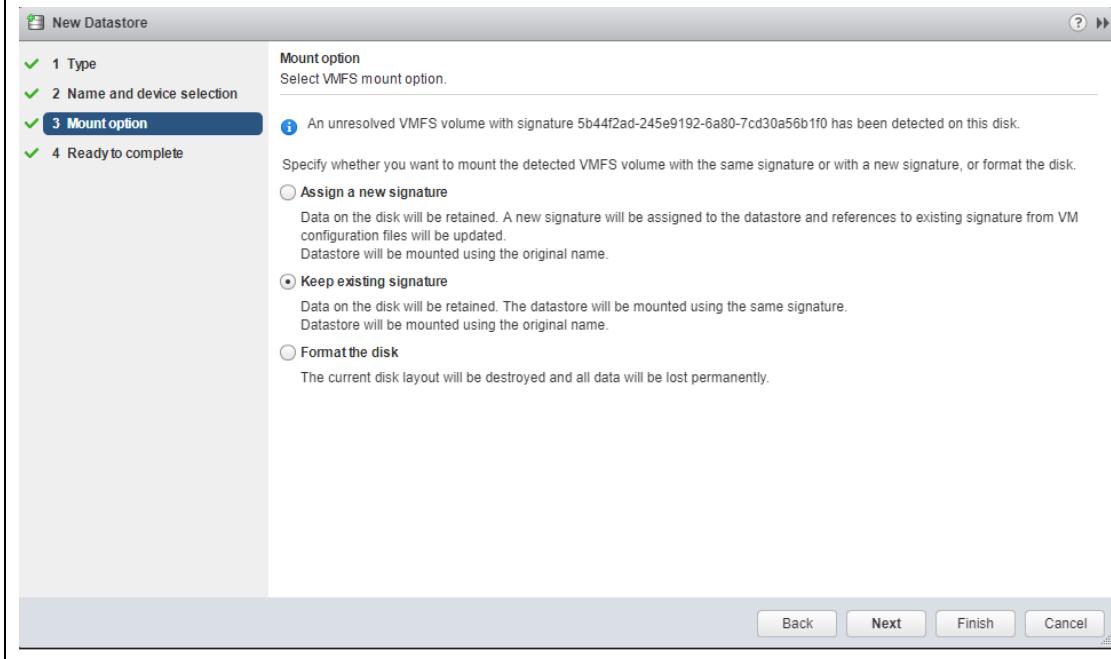
11. Click Next on the location page and Select 'VMFS' for the database type.



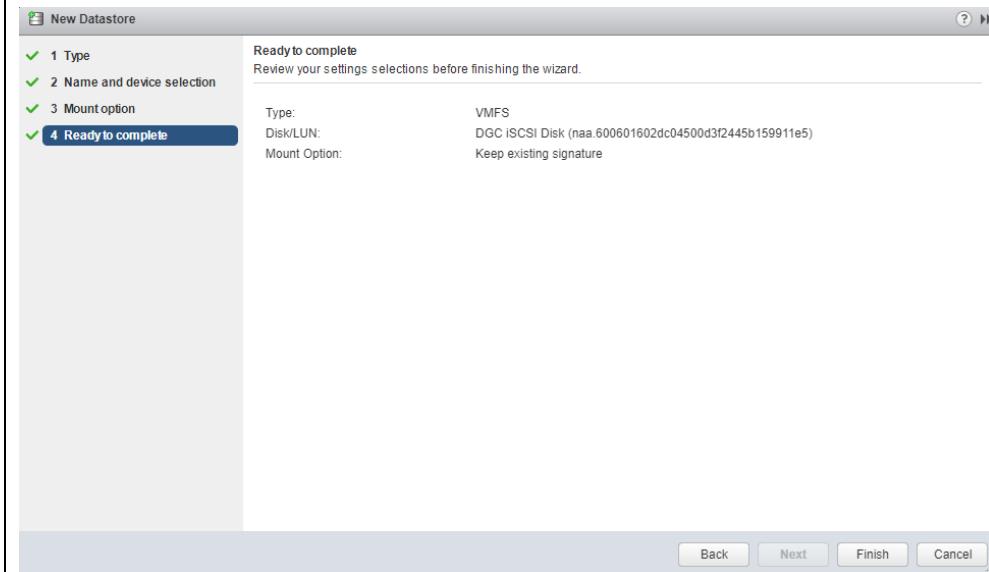
12. Select the disk/LUN listed there and click Next. (the name field can be left as is)



13 Select to ‘Keep the existing signature’.

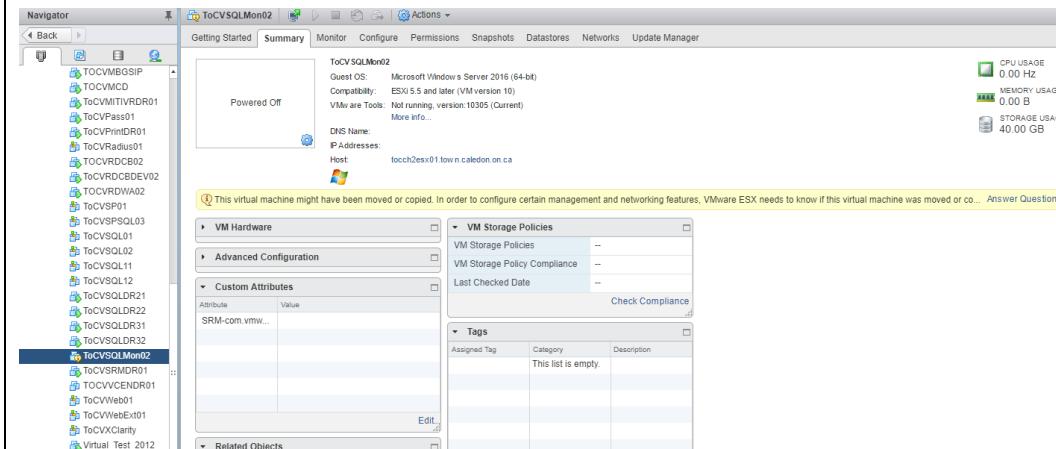


14. Click Finish to complete the wizard.



15. Repeat Steps for additional datastores

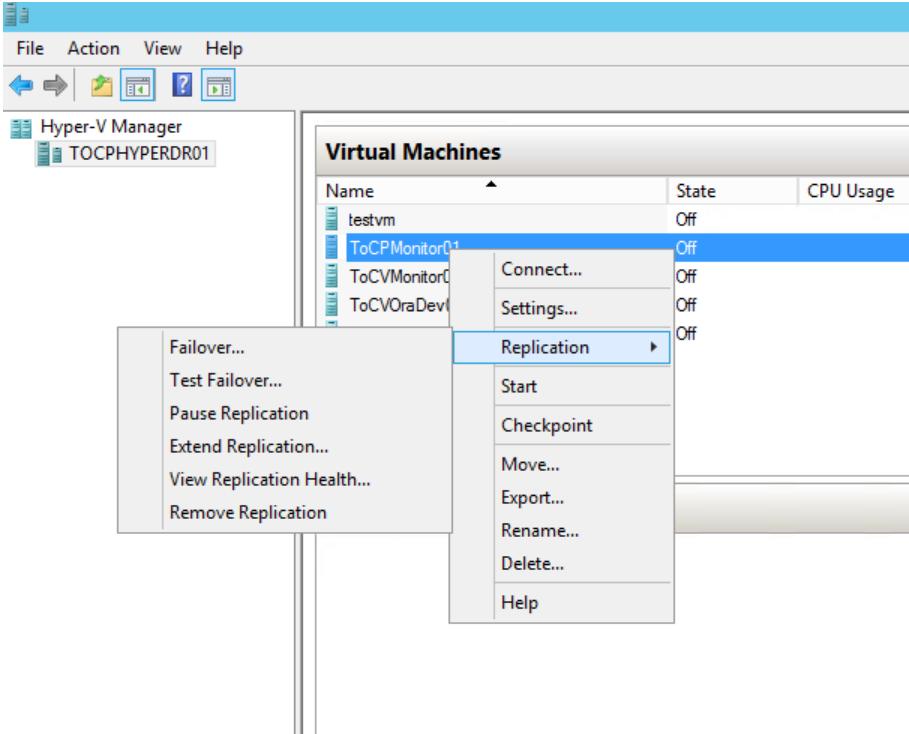
16. Attempt to Power on the VM(s) – At which point you will receive a message asking if the VM was moved or copied.



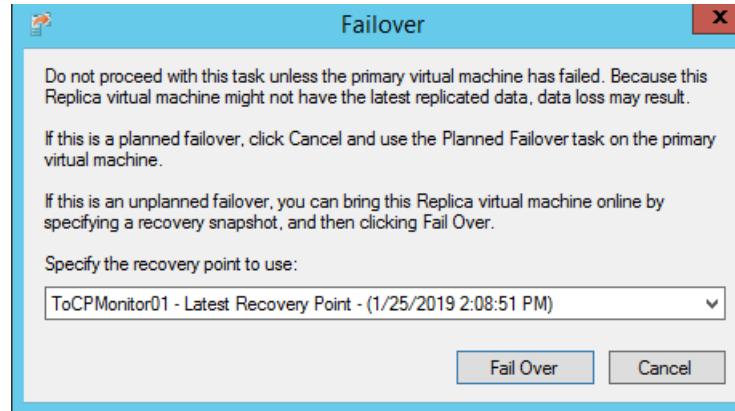
17. Click on answer question.

Select “Moved it”

Hyper-V Failover

| | |
|---|---|
| 1. RDP to the Hyper-V host at DR site | Hostname: TOCPHYPERDR01 IP: 10.2.23.14 |
| 2. Launch Hyper-V Manager | Click start and type 'Hyper-V Manager' |
| 3. Right click on 'ToCPMonitor01' | |
| 4. Click on Failover under Replication. |  <p>The screenshot shows the Windows Start menu with 'Hyper-V Manager' selected. The Hyper-V Manager window is open, displaying a list of virtual machines: testvm, ToCPMonitor01, ToCVMonitor01, and ToCVORADEV. The 'ToCPMonitor01' row is selected. A context menu is open over this machine, with the 'Replication' option highlighted. Other options in the context menu include Failover..., Test Failover..., Pause Replication, Extend Replication..., View Replication Health..., Remove Replication, Connect..., Settings..., Start, Checkpoint, Move..., Export..., Rename..., Delete..., and Help.</p> |

5. Select the Latest Recovery Point and click Fail Over.



Testing

VMware SRM:

1. Confirm you can connect (RDP) to one of the VMs that has been failed over through SRM. E.g. RDP to the email server (Blinky) and confirm it appears to be in a healthy state.

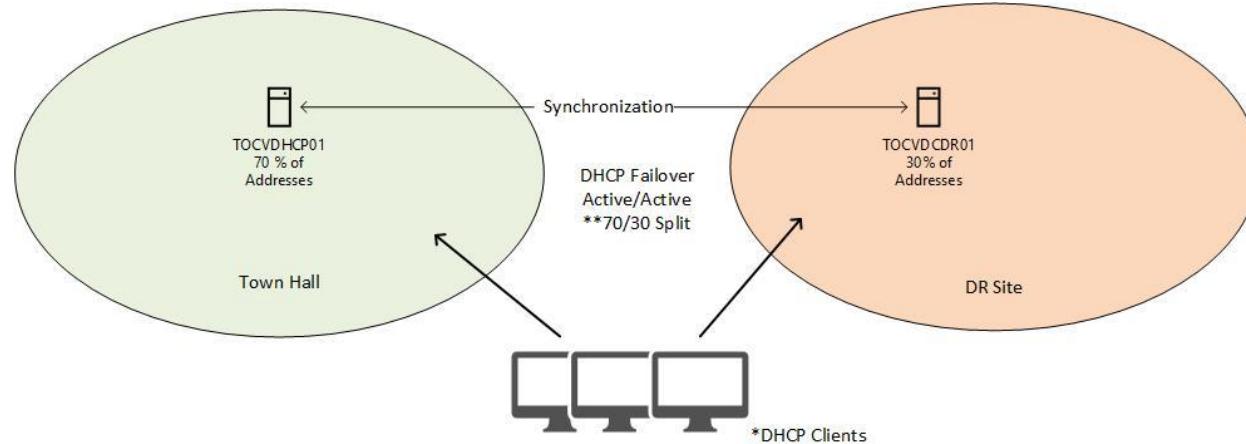
Hyper-V

2. Confirm you can connect (RDP) to one of the VMs that has been failed over through Hyper-V. E.g. RDP to the monitoring server (TOCPMONITOR01) and confirm it appears to be in a healthy state.
3. *Additional application specific testing maybe required for which the application team would need to be engaged.
4. Troubleshooting
5. If you encounter issues during the previous steps, please confirm the physical infrastructure and core services are operational, refer to Appendix L and M.

Appendix M – Core Infrastructure Services Checklist

DHCP

DHCP is setup in a High Availability architecture with a DHCP server at each site (TownHall and DR site) in an active/active configuration. See diagram below for details:



*Only clients with connectivity to both sites would be able to failover between sites.

**Clients at DR site have a 30/70 split with Town Hall and DR site respectively.

In a DR scenario (where the DHCP server at TownHall is unavailable), sites with network connectivity to the DR site should automatically failover to DR site DHCP server.

DNS

Internal DNS

DNS services are integrated with Active Directory – As such they are present on every domain controller in the environment and DNS replication occurs between all domain controller servers as part of AD replication.

The DR site has 2 servers that can provide DNS services.

1. TOCVDCDR01
2. TOCPDCDR01

External DNS

External DNS services are provided by Easy DNS. There is monitoring and failover configured on EasyDNS for the following services. These services will automatically failover to public IPs associated with the DR site internet (Frontier) in case of an outage at Primary site (Sheridan).

| Service/URL | Sheridan IP | Frontier IP (DR Site) |
|----------------------|---------------|-----------------------|
| Eservices.caledon.ca | 142.55.249.40 | 67.21.149.39 |
| ftp.caledon.ca | 142.55.249.37 | 67.21.149.36 |
| Maps.caledon.ca | 142.55.249.39 | 67.21.149.38 |
| Webapp.caledon.ca | 142.55.249.44 | 67.21.149.44 |
| Mail1.caledon.ca | 142.55.249.45 | 67.21.149.43 |

Password Management

In a DR scenario at TownHall, the password management solution should still be accessible via <https://passwordstate.caledon.ca:9119> or <https://10.10.23.2:9119> as the VM resides at the DR site. If you have access to PasswordState, you should be able to login with your regular credentials. If regular credentials are not working, please try the emergency access URL <https://passwordstate.caledon.ca:9119/emergency/>. The emergency login details can be found here.

Networking

Default Route on Switches:

OSPF is used to distribute the default gateway to different sites. In a DR scenario, the DR site core switch should takeover as the default gateway automatically and its default gateway should be the DR site firewall.

Log into the core switch of another site that has a direct fiber connection to DR site (e.g. CCRW) and confirm default route:

| | |
|---|---|
| Log into the CCRW core switch | IP: 172.31.0.49 Username: root Password: **search 2018 switches in password state** |
| Enter enable mode | Type enable password |
| Check routing table | Type “show ip route” |
| The output should indicate DR site core switch as the default gateway (example shown) | Look for the following text: <i>Gateway of last resort is 172.31.0.58 to network 0.0.0.0</i> |

Log into the DR site core switch and confirm default route”

| | |
|--|---|
| Log into the DR site core switch | IP: 172.31.1.2 Username: root Password: **search 2018 switches in password state** |
| Enter enable mode | Type enable password |
| Check routing table | Type “show ip route” |
| The output should indicate DR site firewall as the default gateway (example shown) | Look for the following text: <i>Gateway of last resort is 10.10.0.1 to network 0.0.0.0</i> |

NAT rules on Firewall:

In a DR scenario – access to the Internet should failover to the Frontier (ISP) connection at DR site. The public IP in use for browsing would be 67.21.149.34.

In order for services hosted by the Town to be available through the DR site internet – certain NAT rules need to be disabled on the DR site firewall. These NAT rules allow for DR site to be a tertiary internet backup for services hosted at town hall. But if the servers hosting the services have been moved over to DR site in a disaster recovery scenario, we need to disable these NAT rules, so the rules below it can take over and direct traffic to DR site.

| | |
|--|--|
| Log into the DR site firewall using Putty. Note: You might need to use a jump server if you can't connect directly via VPN. | IP: 10.10.0.1 Username: netadmin Password: ** search ASA firewall in password state** |
| Enter enable mode | Type "enable" on the prompt |
| Enter configuration mode | Type "Conf t" |
| Enter the commands (as shown) to disable the appropriate NAT rules. (Current as of Jan 11, 2018) | <ol style="list-style-type: none"> 1. nat (any,DMZ-TH) source dynamic any interface destination static Outside_67.21.149.36_ftp.caledon.ca DMZ29_ToCVFTPGW01 inactive 2. nat (any,DMZ-TH) source dynamic any interface destination static Outside_67.21.149.38_Fortiweb-ExternalServices DMZ_Fortiweb-ExternalServices_10.0.0.40 inactive 3. nat (any,DMZ-TH) source dynamic any interface destination static Outside_67.21.149.39_Fortiweb-ExternalServicesForceHTTPS DMZ_Fortiweb-ExternalServicesForceHTTPS_10.0.0.41 inactive 4. nat (any,DMZ-TH) source dynamic any interface destination static Outside_67.21.149.44_webapp DMZ_Fortiweb-ExternalServicesForceHTTPS_10.0.0.41 inactive |

ForiWeb (Web Application Firewall)

The WAF is responsible for handling all web related traffic originating externally and some traffic originating internally. It plays a critical role in providing access to web applications.

There is a HA pair of FortiWeb WAFs at Town Hall and a single virtual Fortiweb WAF at DR site. At this time the configuration is not pushed from TH WAFs to the WAF at DR site.

Manual configuration is required on WAF at DR site in order to enable services in a DR scenario. This section will be updated once the configuration of DR site WAF has been updated to allow for more automated failover and a process has been put in place to sync the configuration.

Appendix N – Physical Infrastructure Checklist

Note: Passwords can be found in PasswordState: <https://passwordstate.caledon.ca:9119> (For more details on PasswordState refer to Appendix L)

If you are unable to connect to any of these devices, it could be due to the following and could require a visit to the DR site to troubleshoot further:

1. Network connectivity
2. Device offline/ service unavailable

| Device | Steps to check | Location |
|------------------|---|----------|
| Switches | Open a Terminal Emulator program (e.g. Putty) and confirm you can SSH and log into the following switches at DR site. 172.31.1.2 (4500 core Switch) 10.10.8.3 (2960X switch) | DR Site |
| Firewall | If you are able to VPN to the DR site firewall using steps in Appendix B then firewall itself is up and operational. If on-site, you should be able to SSH to the firewall using IP 10.10.0.1 | DR Site |
| Backup Appliance | Confirm you can log into the Unitrends Backup Appliance through https://t0cpunitrends2/ui/#/ or https://10.2.22.2 Note: the appliance utilizes local authentication only. | DR Site |
| Server Chassis | Confirm Server Chassis is operational by connecting to the onboard CMM. https://10.10.8.10 using recovery_id. | DR Site |
| Physical Servers | RDP to TOCPDCDR01 (10.10.22.18) RDP to TOCPHYPERDR01 (10.2.23.14). Browse to | DR Site |
| SAN | Confirm you can connect to the DR site SAN and it is operational. https://unity-dr | DR Site |

Appendix O – Primary Data Centre Failback Procedures

Failback to Town Hall

This document is intended to be a guide on restoring services at the Primary Data Center (Town Hall) after a failover to DR site has occurred.

Assumptions:

1. The Primary Data Center is in a state to start hosting services again and services are being reverted to the original systems (physical and logical).
2. Additional steps could be required if systems at the Primary Data Center had to be replaced (e.g. new SAN or Server Chassis). This guide doesn't cover those steps.

The following is an overview of the steps that need to be taken:

1. Shutdown of certain services at DR-Site
2. Power On equipment at Town Hall (SAN, Chassis, Switch)
3. Failback vCenter Server
4. Revert Telephone system
5. Revert Email System
6. Revert Databases
7. Revert File Shares
8. Revert Software Defined Infrastructure (VMware, Hyper-V)
9. Bring services online

Step 1 - Shutdown of Services at DR Site

VMware

We will be shutting down VMs that were manually migrated to the DR site in the original failover. Shutdown all VMs that reside on Datastores migrated from Town Hall. Below is the list of datastores (at the time of writing):

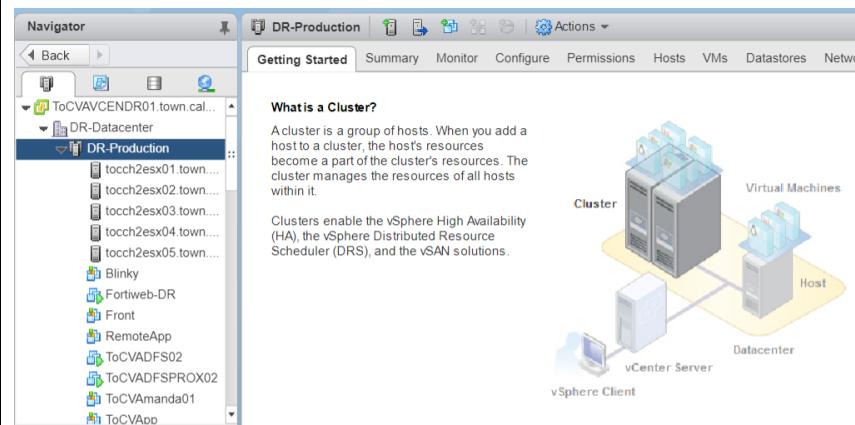
- DS-1Hour-01
- DS-1Hour-02
- DS-1Hour-03
- DS-1Hour-04
- DS-5Min-01

1. Open a web browser and browse to: <https://tocvavcndr01>

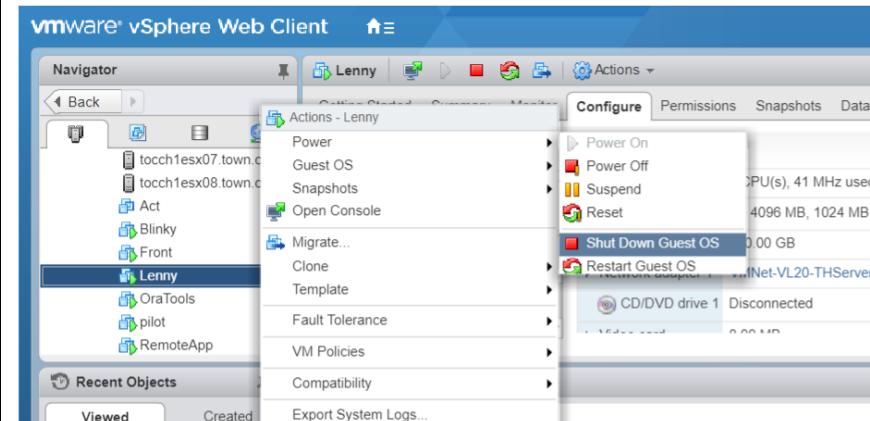
2. Click on vSphere Web Client (Flash)

3. Login with your domain admin account

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**

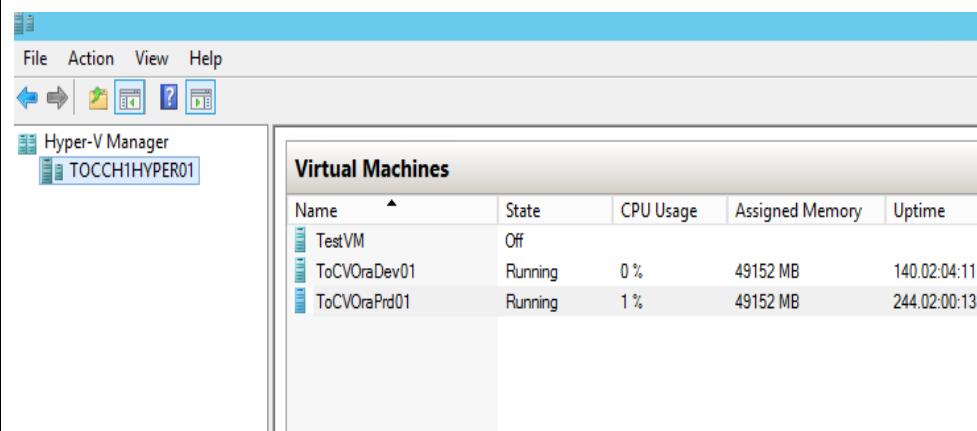


Hyper-V

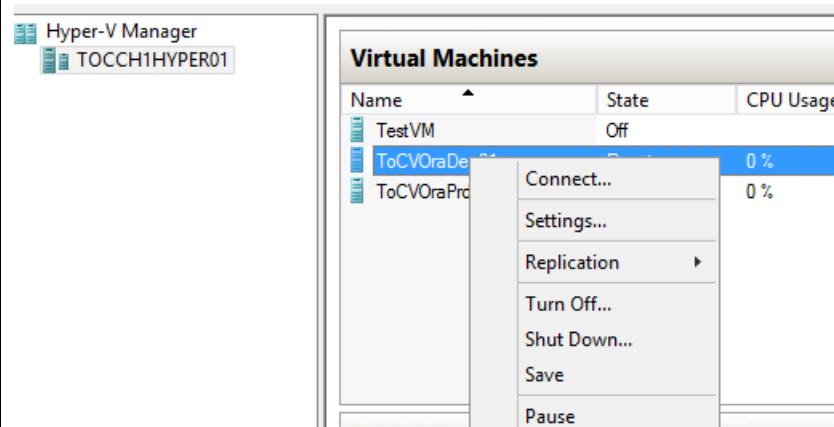
1. RDP to hyper-v host at DR site.

Server name: **TOCCH1HYPERDR01**

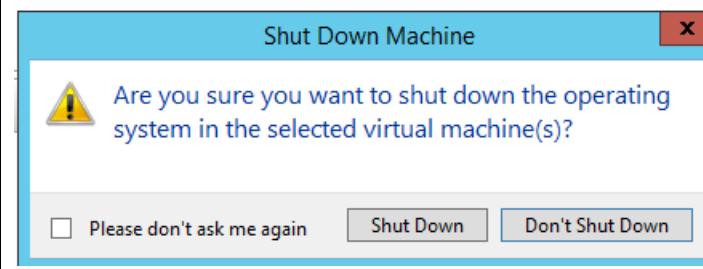
2. Launch 'Hyper-V Manager'



3. Right click the VM you wish to shutdown and click **Shut Down**.



4. Click **Shutdown** again to confirm



Step 2 - Failback vCenter Server

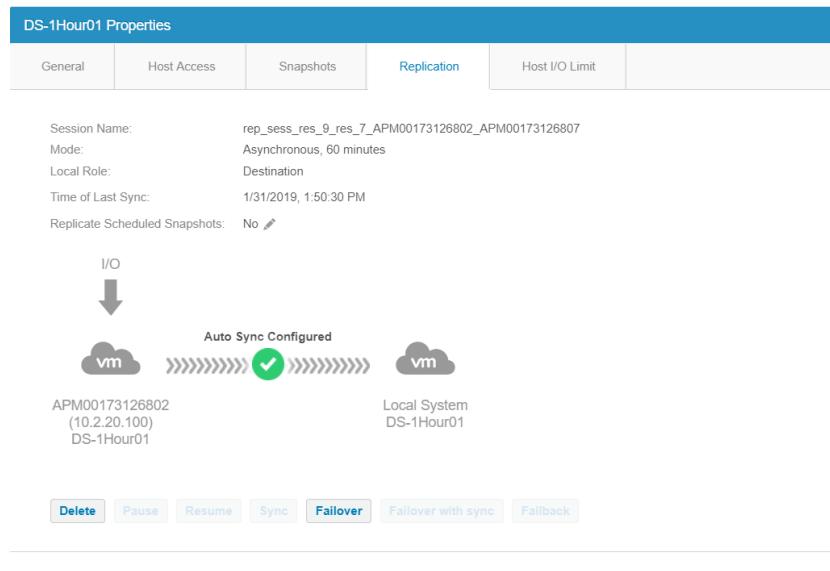
If the Datastore hosting the Town Hall vCenter server was failed over during a DR scenario - We will need to failback it back so the Town Hall VMware environment can start hosting services again and can be managed through a vCenter.

| 1. Identify the Datastore hosting ToCVACEN01 | From the DR site VMware environment identify the datastore hosting ToCVACEN01 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|--|--|---------------|-----------|---------------|----------|-------------|---------|-----|-----|-------------|---------|-----|-----|-------------|---------|-----|-----|-------------|---------|-----|-----|------------|---------|-----|-----|--------------|---------|-----|-----|--------------|---------|-----|-----|---------------|-------|-----|-----|--------------------|-------|-----|-----|----------------|---------|-----|-----|----------------|---------|-----|-----|---------------------|---------|-----|-----|----------------------|------|-----|-----|-------------------------|------|-----|-----|---------------|-------|-----|-----|-------------|-------|-----|-----|-------------|-------|-----|-----|-------------|-------|-----|-----|
| 2. After confirming no machines are running on the datastores Failback the Datastores through the DR site SAN. | <p>Log into Unity-DR SAN (https://unity-dr) and failback all Datastores that were previously failed over. See list below for reference:</p> <ul style="list-style-type: none"> - DS-1Hour-01 - DS-1Hour-02 - DS-1Hour-03 - DS-1Hour-04 - DS-5Min-01 <table border="1"> <thead> <tr> <th>Name</th> <th>Size (GB)</th> <th>Allocated (%)</th> <th>Used (%)</th> </tr> </thead> <tbody> <tr><td>DS-1Hour-01</td><td>3,584.0</td><td>---</td><td>---</td></tr> <tr><td>DS-1Hour-03</td><td>3,584.0</td><td>---</td><td>---</td></tr> <tr><td>DS-1Hour-02</td><td>3,584.0</td><td>---</td><td>---</td></tr> <tr><td>DS-1Hour-04</td><td>3,584.0</td><td>---</td><td>---</td></tr> <tr><td>DS-5Min-01</td><td>2,560.0</td><td>---</td><td>---</td></tr> <tr><td>DS-5MinSRM01</td><td>2,560.0</td><td>---</td><td>---</td></tr> <tr><td>DS-5MinSRM02</td><td>3,072.0</td><td>---</td><td>---</td></tr> <tr><td>DS-5MinSRM-03</td><td>200.0</td><td>---</td><td>---</td></tr> <tr><td>DS-DR->TH5MinRep01</td><td>400.0</td><td>---</td><td>---</td></tr> <tr><td>DS-DR-NoRep-01</td><td>1,024.0</td><td>---</td><td>---</td></tr> <tr><td>DS-DR-NoRep-02</td><td>1,024.0</td><td>---</td><td>---</td></tr> <tr><td>DS-DR-NoRep-Archive</td><td>1,024.0</td><td>---</td><td>---</td></tr> <tr><td>DS-DR-SRMPlaceholder</td><td>10.0</td><td>---</td><td>---</td></tr> <tr><td>DS-DR-SRMPlaceholder-01</td><td>10.0</td><td>---</td><td>---</td></tr> <tr><td>DS-DR-TestDev</td><td>505.0</td><td>---</td><td>---</td></tr> <tr><td>DS-DR-VCEN6</td><td>100.0</td><td>---</td><td>---</td></tr> <tr><td>DS-SRM-Test</td><td>100.0</td><td>---</td><td>---</td></tr> <tr><td>DS-Test-Dev</td><td>500.0</td><td>---</td><td>---</td></tr> </tbody> </table> | Name | Size (GB) | Allocated (%) | Used (%) | DS-1Hour-01 | 3,584.0 | --- | --- | DS-1Hour-03 | 3,584.0 | --- | --- | DS-1Hour-02 | 3,584.0 | --- | --- | DS-1Hour-04 | 3,584.0 | --- | --- | DS-5Min-01 | 2,560.0 | --- | --- | DS-5MinSRM01 | 2,560.0 | --- | --- | DS-5MinSRM02 | 3,072.0 | --- | --- | DS-5MinSRM-03 | 200.0 | --- | --- | DS-DR->TH5MinRep01 | 400.0 | --- | --- | DS-DR-NoRep-01 | 1,024.0 | --- | --- | DS-DR-NoRep-02 | 1,024.0 | --- | --- | DS-DR-NoRep-Archive | 1,024.0 | --- | --- | DS-DR-SRMPlaceholder | 10.0 | --- | --- | DS-DR-SRMPlaceholder-01 | 10.0 | --- | --- | DS-DR-TestDev | 505.0 | --- | --- | DS-DR-VCEN6 | 100.0 | --- | --- | DS-SRM-Test | 100.0 | --- | --- | DS-Test-Dev | 500.0 | --- | --- |
| Name | Size (GB) | Allocated (%) | Used (%) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| DS-1Hour-01 | 3,584.0 | --- | --- | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| DS-1Hour-03 | 3,584.0 | --- | --- | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| DS-1Hour-02 | 3,584.0 | --- | --- | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| DS-1Hour-04 | 3,584.0 | --- | --- | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| DS-5Min-01 | 2,560.0 | --- | --- | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| DS-5MinSRM01 | 2,560.0 | --- | --- | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| DS-5MinSRM02 | 3,072.0 | --- | --- | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| DS-5MinSRM-03 | 200.0 | --- | --- | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| DS-DR->TH5MinRep01 | 400.0 | --- | --- | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| DS-DR-NoRep-01 | 1,024.0 | --- | --- | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| DS-DR-NoRep-02 | 1,024.0 | --- | --- | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| DS-DR-NoRep-Archive | 1,024.0 | --- | --- | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| DS-DR-SRMPlaceholder | 10.0 | --- | --- | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| DS-DR-SRMPlaceholder-01 | 10.0 | --- | --- | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| DS-DR-TestDev | 505.0 | --- | --- | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| DS-DR-VCEN6 | 100.0 | --- | --- | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| DS-SRM-Test | 100.0 | --- | --- | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| DS-Test-Dev | 500.0 | --- | --- | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

- 3. Click on the edit icon and under Replication click on Fallback.**

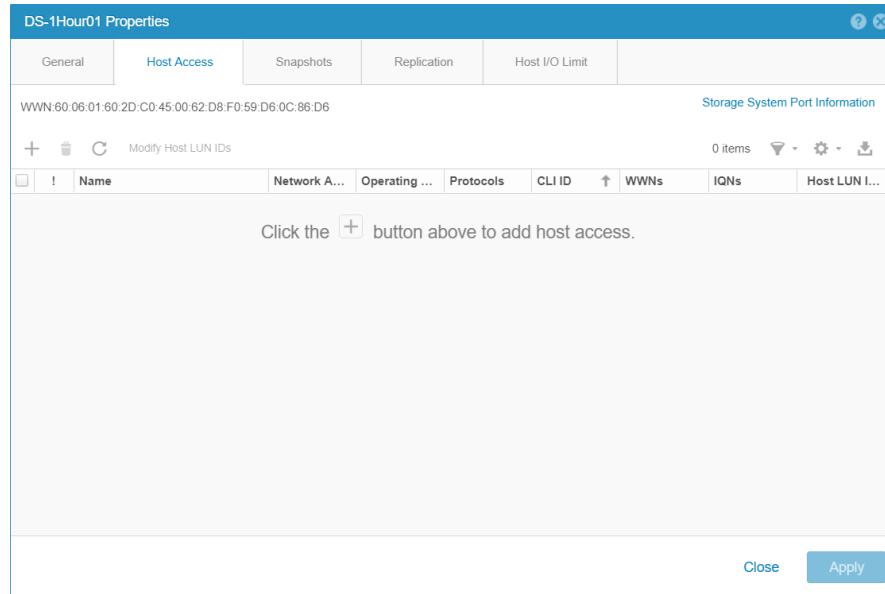
Do this for all datastores that need to be failed back

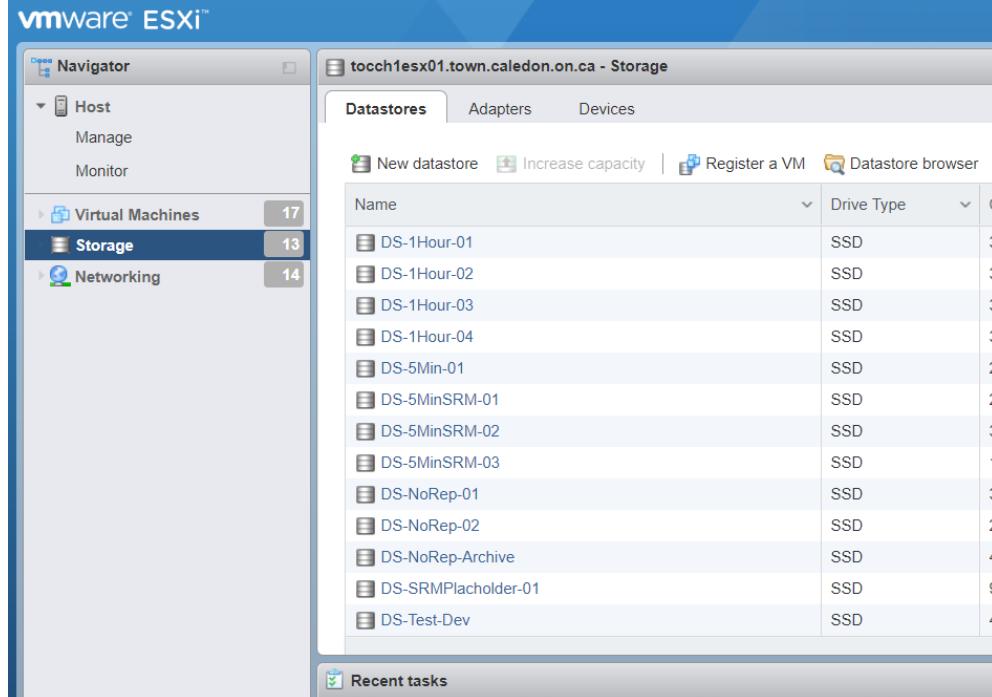
**Greyed out in this screenshot*



- 4. On the Town Hall SAN confirm the VMware hosts have access to the datastore that has been failed back.**

If they don't have access – add them under host access.



| <p>5. Directly connect to a host at Town Hall which has access from the previous step. e.g tocch1esx01</p> | <p>You can directly connect to a host by typing its IP address on the web browser. User local login credentials (available in password state).</p> | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|--|------|------------|---|-------------|-----|---|-------------|-----|---|-------------|-----|---|-------------|-----|---|------------|-----|---|---------------|-----|---|---------------|-----|---|---------------|-----|---|-------------|-----|---|-------------|-----|---|------------------|-----|---|-----------------------|-----|---|-------------|-----|---|
| <p>6. Confirm you can connect to the datastore which was identified as hosting the vcenter server (in Step 1)</p> <p>If its present under storage. Add it through "New Datastore"</p> |  <table border="1" data-bbox="1157 486 1797 943"> <thead> <tr> <th>Name</th> <th>Drive Type</th> <th>C</th> </tr> </thead> <tbody> <tr><td>DS-1Hour-01</td><td>SSD</td><td>3</td></tr> <tr><td>DS-1Hour-02</td><td>SSD</td><td>3</td></tr> <tr><td>DS-1Hour-03</td><td>SSD</td><td>3</td></tr> <tr><td>DS-1Hour-04</td><td>SSD</td><td>3</td></tr> <tr><td>DS-5Min-01</td><td>SSD</td><td>2</td></tr> <tr><td>DS-5MinSRM-01</td><td>SSD</td><td>2</td></tr> <tr><td>DS-5MinSRM-02</td><td>SSD</td><td>3</td></tr> <tr><td>DS-5MinSRM-03</td><td>SSD</td><td>1</td></tr> <tr><td>DS-NoRep-01</td><td>SSD</td><td>3</td></tr> <tr><td>DS-NoRep-02</td><td>SSD</td><td>2</td></tr> <tr><td>DS-NoRep-Archive</td><td>SSD</td><td>4</td></tr> <tr><td>DS-SRMPPlaceholder-01</td><td>SSD</td><td>9</td></tr> <tr><td>DS-Test-Dev</td><td>SSD</td><td>4</td></tr> </tbody> </table> | Name | Drive Type | C | DS-1Hour-01 | SSD | 3 | DS-1Hour-02 | SSD | 3 | DS-1Hour-03 | SSD | 3 | DS-1Hour-04 | SSD | 3 | DS-5Min-01 | SSD | 2 | DS-5MinSRM-01 | SSD | 2 | DS-5MinSRM-02 | SSD | 3 | DS-5MinSRM-03 | SSD | 1 | DS-NoRep-01 | SSD | 3 | DS-NoRep-02 | SSD | 2 | DS-NoRep-Archive | SSD | 4 | DS-SRMPPlaceholder-01 | SSD | 9 | DS-Test-Dev | SSD | 4 |
| Name | Drive Type | C | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| DS-1Hour-01 | SSD | 3 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| DS-1Hour-02 | SSD | 3 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| DS-1Hour-03 | SSD | 3 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| DS-1Hour-04 | SSD | 3 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| DS-5Min-01 | SSD | 2 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| DS-5MinSRM-01 | SSD | 2 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| DS-5MinSRM-02 | SSD | 3 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| DS-5MinSRM-03 | SSD | 1 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| DS-NoRep-01 | SSD | 3 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| DS-NoRep-02 | SSD | 2 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| DS-NoRep-Archive | SSD | 4 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| DS-SRMPPlaceholder-01 | SSD | 9 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| DS-Test-Dev | SSD | 4 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| <p>7. ADDITIONAL STEPS NEEDED</p> | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

Step 3 – Telephone System

The following should failback automatically once network connectivity has been restored between Townhall and DR site and Town Hall and SIP provider.

- The main phone number for Caledon (905-574-2272) should failback automatically to Town Hall.
- Phones at sites with connectivity to DR site should automatically failback to phone controller at Town Hall.

The following steps need to be done manually:

- Need to failback a VM named TOCVMAS01 (Voicemail/AutoAttendant) from the DR site through VMware SRM.
- For steps on SRM failover, refer to Appendix X and use '**Mitel_Prod_ProtectionGroup**' as the group being failed over.

Step 4 - Email

The email system is provided through O365. Mailboxes reside in O365 and mail routing is done through O365. Users simply need an internet connection in order to access email.

External DNS provider (EasyDNS) should automatically failover the dns records required to maintain mail flow to O365.

Exception:

The only exception to this is systems that rely on internal mail relay e.g. If an application sends an email internally or externally, it would connect to the on-premise exchange server. The exchange server (Blinky) will need to be failed back to Town Hall through SRM.

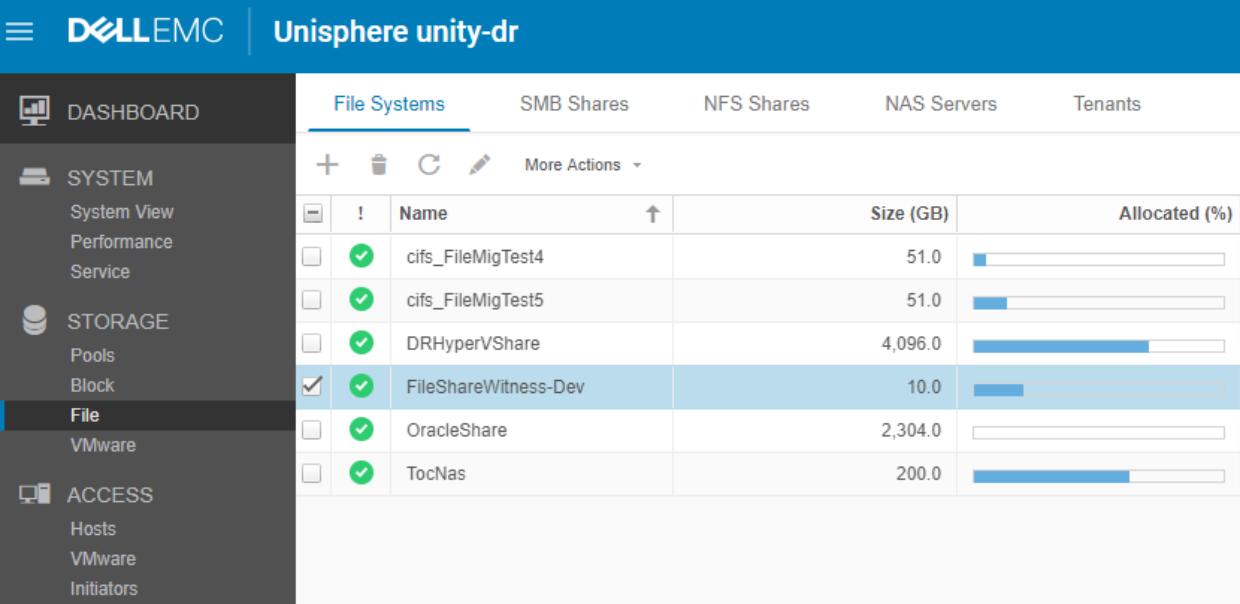
Refer to **Annex X** and use '**Prod_ProtectionGroup**' as the group being failed over.

Important: Don't failover 'Prod_ProtectionGroup' until you **have completed Step X (Database Recovery)** in the failback table. Initiating the failback will power on the VMs at the Town Hall site which would require the Databases to be available first, in order for the application to function.

Step 5 – Database Failback

SQL

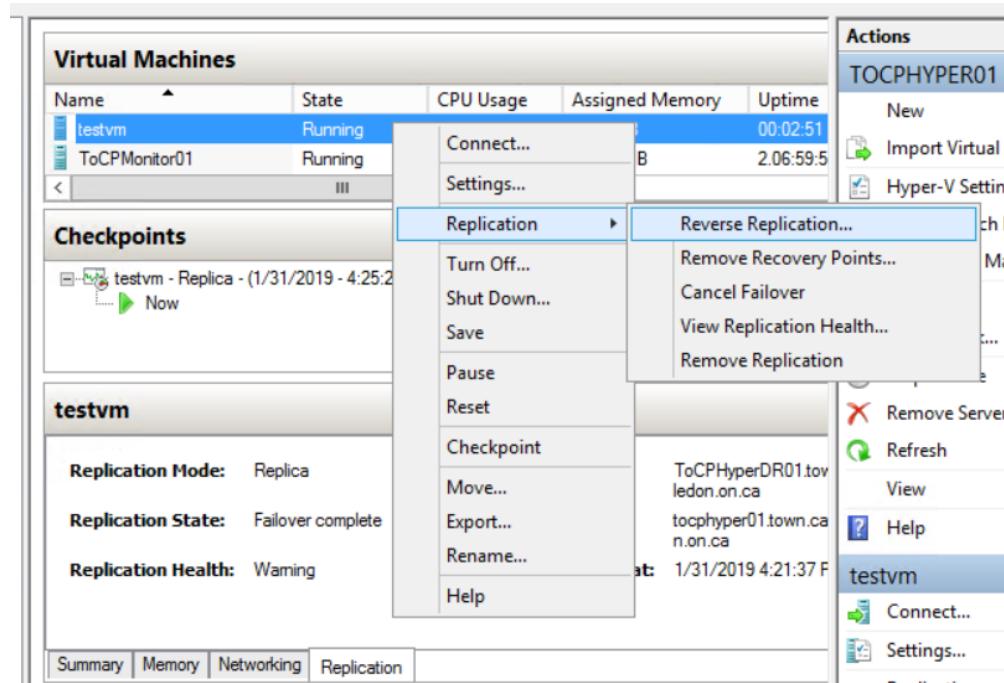
- | | |
|---|--|
| 1. Shutdown all active cluster nodes utilizing FileShare witness at DR site | At the time of writing the following nodes rely on the production file share witness: <ul style="list-style-type: none">- TOCVFILEDR01- TOCFILEDR02- TOCVSQQLDR31- TOCVSQQLDR32 |
|---|--|

| | <ul style="list-style-type: none"> - TOCVDQLDR22 - TOCVDQLDR21 | | | | | | | | | | | | | | | | | | | | | |
|-----------------------------|--|---------------|-----------|---------------|-------------------|------|----|-------------------|------|-----|---------------|---------|-----|-----------------------------|------|-----|-------------|---------|-----|--------|-------|-----|
| 2. | From the left menu click on File under the Storage heading. | | | | | | | | | | | | | | | | | | | | | |
| 3. | <p>Select the FileShareWitness-Prod File System and click the edit icon.</p>  <table border="1"> <thead> <tr> <th>Name</th> <th>Size (GB)</th> <th>Allocated (%)</th> </tr> </thead> <tbody> <tr> <td>cifs_FileMigTest4</td> <td>51.0</td> <td>5%</td> </tr> <tr> <td>cifs_FileMigTest5</td> <td>51.0</td> <td>10%</td> </tr> <tr> <td>DRHyperVShare</td> <td>4,096.0</td> <td>80%</td> </tr> <tr> <td>FileShareWitness-Dev</td> <td>10.0</td> <td>10%</td> </tr> <tr> <td>OracleShare</td> <td>2,304.0</td> <td>10%</td> </tr> <tr> <td>TocNas</td> <td>200.0</td> <td>10%</td> </tr> </tbody> </table> | Name | Size (GB) | Allocated (%) | cifs_FileMigTest4 | 51.0 | 5% | cifs_FileMigTest5 | 51.0 | 10% | DRHyperVShare | 4,096.0 | 80% | FileShareWitness-Dev | 10.0 | 10% | OracleShare | 2,304.0 | 10% | TocNas | 200.0 | 10% |
| Name | Size (GB) | Allocated (%) | | | | | | | | | | | | | | | | | | | | |
| cifs_FileMigTest4 | 51.0 | 5% | | | | | | | | | | | | | | | | | | | | |
| cifs_FileMigTest5 | 51.0 | 10% | | | | | | | | | | | | | | | | | | | | |
| DRHyperVShare | 4,096.0 | 80% | | | | | | | | | | | | | | | | | | | | |
| FileShareWitness-Dev | 10.0 | 10% | | | | | | | | | | | | | | | | | | | | |
| OracleShare | 2,304.0 | 10% | | | | | | | | | | | | | | | | | | | | |
| TocNas | 200.0 | 10% | | | | | | | | | | | | | | | | | | | | |

| | |
|---|--|
| <p>4. Click on the Replication tab and click Failback to initiate the process.</p> | |
| <p>5. The failback process can take some time as it will sync between DR site to Town Hall and then failback.</p> | <p>Note: the “Filesharewitness-prod” DNS record has a TTL of 5 mins so it can take that long for the file share witness to be accessible through the new IP address at Town Hall site.</p> |
| <p>6. Power on the servers in the SQL cluster at TH first and then DR site.</p> | <p>The following SQL server cluster nodes exist at Town Hall:</p> <ul style="list-style-type: none"> - TOCYSQL31 - TOCYSQL32 - TOCYSQL21 - TOCYSQL22 <p>The following SQL cluster nodes exist at DR site:</p> <ul style="list-style-type: none"> - TOCVSQLDR31 - TOCVSQLDR32 - TOCVSQLDR22 - TOCVSQLDR21 |

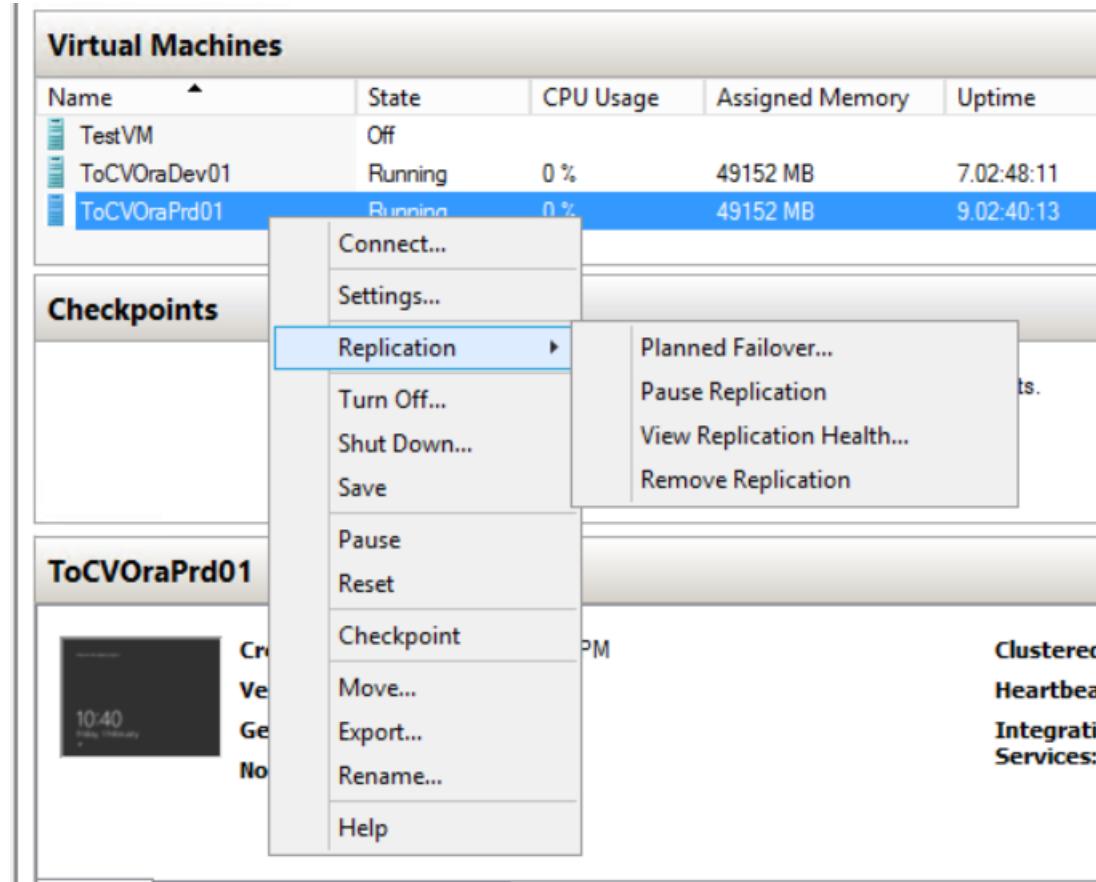
| | |
|--|---|
| | |
| 7. Connect to a SQL server cluster node and check health | Connect to the appropriate SQL server at the TH and launch Failover Cluster Manager to confirm health of the cluster. |
| 8. Check health and connectivity. | Have a member of the database team check the health and connectivity to the databases residing on the cluster in question. Note: A reboot of all the nodes in the cluster maybe required |
| 9. Repeat steps for other SQL clusters as needed. | |
| Oracle | |
| Oracle databases servers run in a clustered Hyper-V environment, with a host at each site (Townhall and DR site). In a Failback scenario, we will connect to the DR site host and first reverse replication of the VM (DR to Town Hall). | |
| 1. RDP to the Hyper-V host at DR site | Hostname: TOCPHYPERDR01 IP: 10.2.23.14 |
| 2. Launch Hyper-V Manager | Click start and type 'Hyper-V Manager' |
| 3. Right click on ToCVoraPrd01 | |

4. Click on **Reverse Replicaiton** under **Replication**.



5. Follow the wizard to configure replication from DR site to Town Hall

6. Once replication is setup
– perform a **Planned Failover**.



7. **ToCVOraprd01** should now be running at Town Hall.

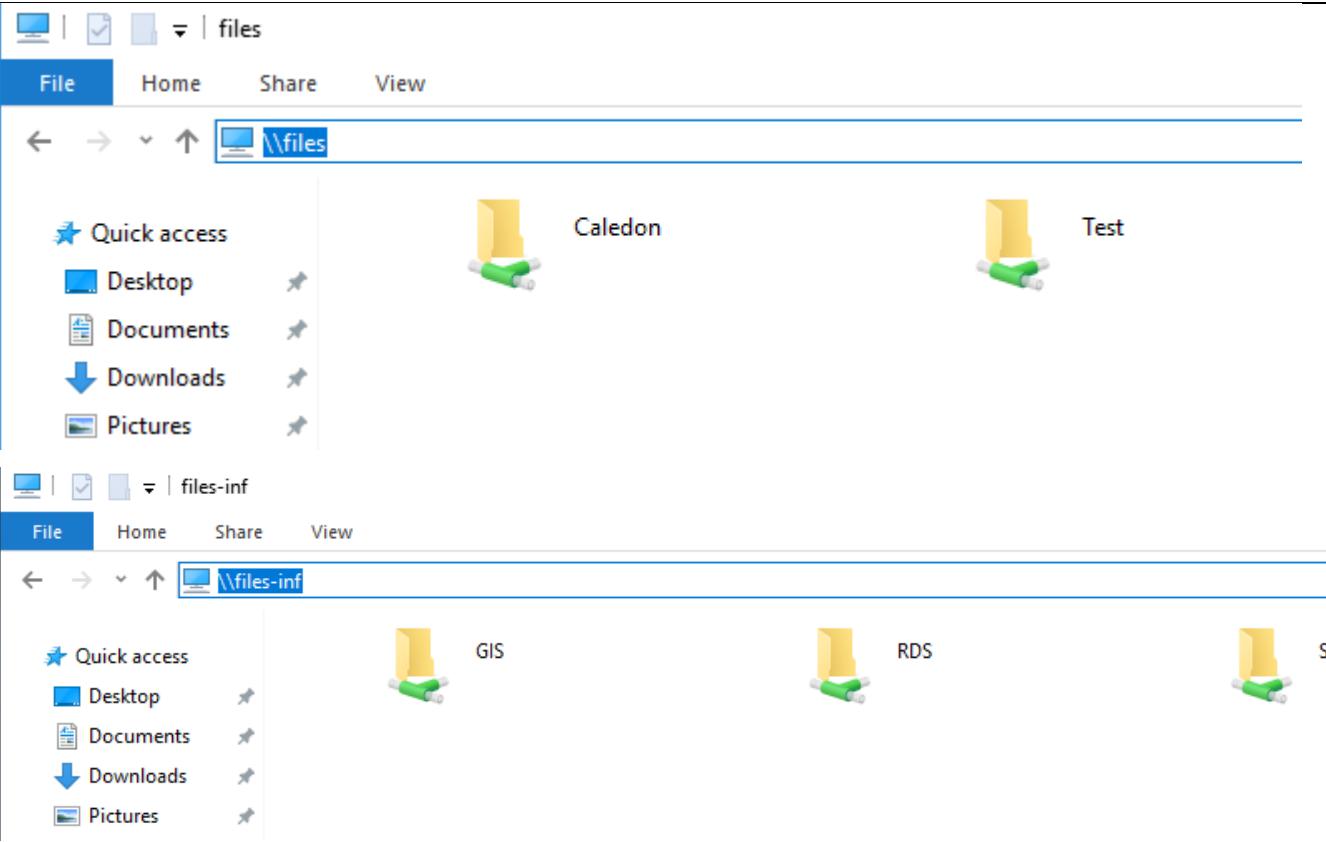
Confirm connectivity and health of the VM.
Have the database team confirm the health and connectivity to the Oracle database.

Step 5 - File System

Fallback Windows File Server Cluster

| 1. Ensure the cluster witness share has already been failed-back. | Ensure that steps 1 – 4 for SQL Database Recovery have already been completed and the ' FileShareWitness-Prod ' has already been failed back to Town Hall. | | | | | | | | | | | | | | | | | | |
|---|---|-------------|------------|----------|-------------|----------|-------------|-------|---------|-------------|------------|--------|--|-----------|---------|-------------|------------|------|--|
| 2. Power-on File server cluster nodes | <p>Power-on file server cluster nodes at Town Hall and DR site:</p> <ul style="list-style-type: none"> - TOCVFILE01 - TOCVFILE02 - TOCVFILEDR01 - TOCVFILEDR02 | | | | | | | | | | | | | | | | | | |
| 3. Connect to one of the nodes at TH and check health | Launch Failover Cluster Manager and confirm health of cluster and visibility of the file share witness. | | | | | | | | | | | | | | | | | | |
| 4. Connect to one of the nodes at TH and check health | Launch Failover Cluster Manager and confirm health of cluster and visibility of the file share witness. | | | | | | | | | | | | | | | | | | |
| 5. Expand the cluster object and click on Roles | <table border="1"> <thead> <tr> <th>Name</th> <th>Status</th> <th>Type</th> <th>Owner Node</th> <th>Priority</th> <th>Information</th> </tr> </thead> <tbody> <tr> <td>Files</td> <td>Running</td> <td>File Server</td> <td>TOCVFile01</td> <td>Medium</td> <td></td> </tr> <tr> <td>Files-inf</td> <td>Running</td> <td>File Server</td> <td>TOCVFile02</td> <td>High</td> <td></td> </tr> </tbody> </table> | Name | Status | Type | Owner Node | Priority | Information | Files | Running | File Server | TOCVFile01 | Medium | | Files-inf | Running | File Server | TOCVFile02 | High | |
| Name | Status | Type | Owner Node | Priority | Information | | | | | | | | | | | | | | |
| Files | Running | File Server | TOCVFile01 | Medium | | | | | | | | | | | | | | | |
| Files-inf | Running | File Server | TOCVFile02 | High | | | | | | | | | | | | | | | |
| 6. Confirm the roles are running | Confirm the ' Files ' and ' Files-inf ' roles are running on TOCVFILE01 and TOCVFILE02. If not, attempt to move the roles over to those nodes. | | | | | | | | | | | | | | | | | | |

7. Confirm the file share(s) can be accessed through Windows Explorer.



Steps to Failover FileShares on EMC VNX (Coltrane)

1. Connect to EMC VNX SAN at DR site.

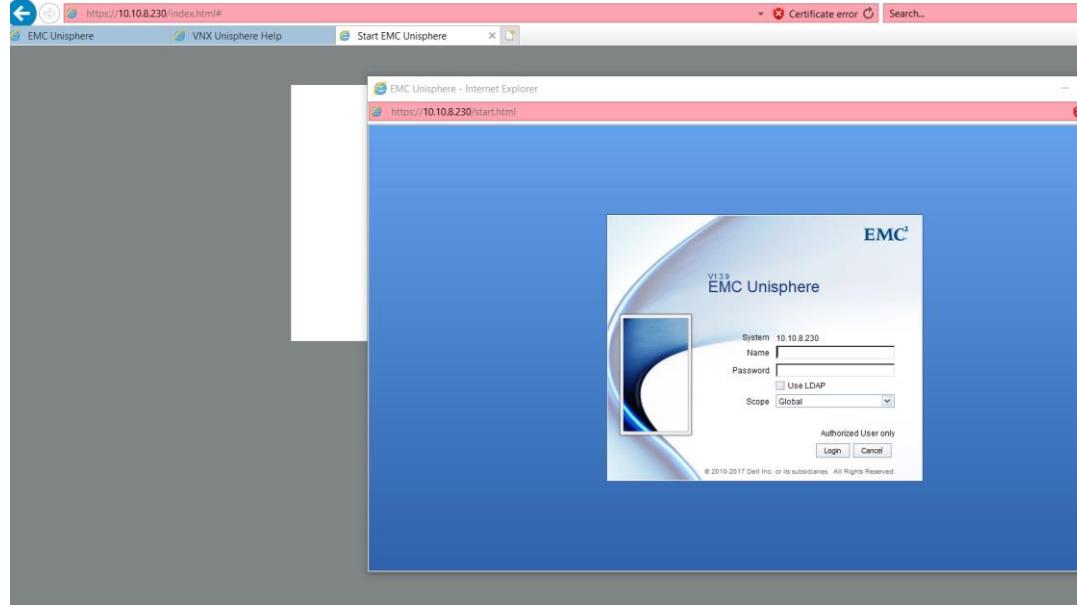
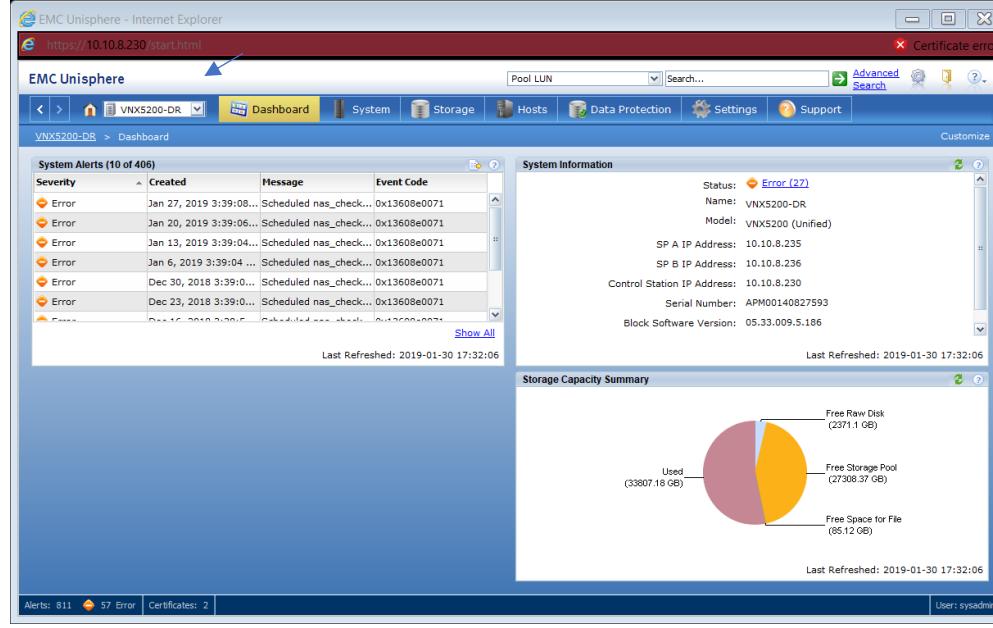
<https://10.10.8.230>

Note: The web application requires Java. You will likely need to add the IP address to trusted sites under Java Exception site list (from the control panel). Additionally, there are several security related pop-ups and warnings that must be accepted to get to the login screen.

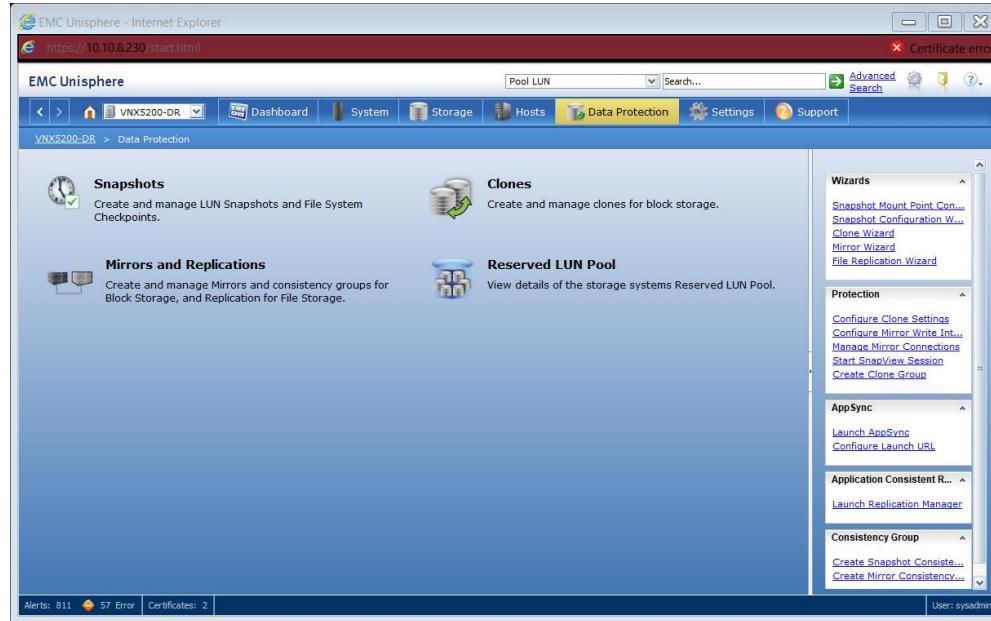
2. Enter the credentials

Credentials can be found in PasswordState

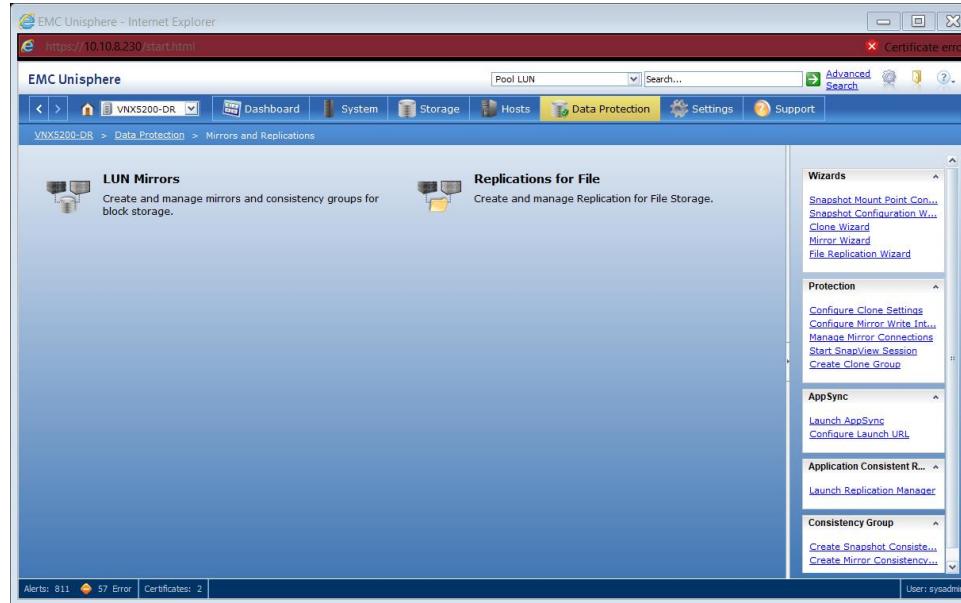
Town of Caledon Disaster Recovery Playbook – Administration Building Data Center

| | |
|--|---|
| |  |
| <p>3. Select VNX5200-DR from the drop down menu.</p> |  |

4. Click on **Data Protection** and then **Mirrors and Replications**



5. Click on **Replications for File**



- 6. First select **cifs_dm1_replica2018** and then click on Reverse**

Once the data mover is failed back we can move the file system.

Select:
cifs_Coltrane_FS_Replication and then click **Reverse**

| Name | Local Object | Local Data Mover | Data Mover Inter... | Remote System | Status |
|-------------------------|--------------------|------------------|---------------------|---------------|--------|
| cifs_Coltrane_FS_Rep... | cifs_Coltrane | server_2 | DR_DM_Inter... | Prod-CS0 | OK |
| cifs_dm1_replica2018 | cifs_vdm1_replica1 | server_2 | DR_DM_Inter... | Prod-CS0 | OK |

- 7. Once replication is synced in the reverse direction. Select **cifs_dm1_replica2018** and click **Switchover**.**

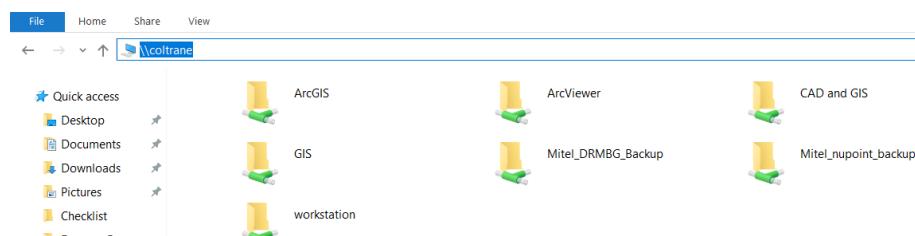
Repeat for:
cifs_Coltrane_FS_Replication.

- 8. Once failed over DNS might need a manual update.**

Go to TOCVDCDR01 and Open DNS and see if Coltrane now points to "172.20.0.232". If not modify the A record for Coltrane as needed.

Note: The TTL for Coltrane is set to 20 mins so it could take up to 20 mins before clients will get the updated DNS record.

9. Connect to the 'Coltrane' file share through Windows Explorer to confirm its accessible.



Software-Defined Infrastructure Failback

VMware (SRM) Failover Procedure

1. Connect to DR site VM

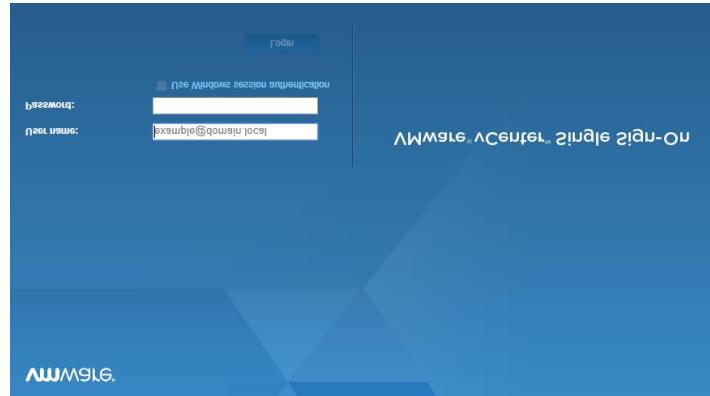
2. Open a web browser and browse to:

<https://tocvavcendr01>

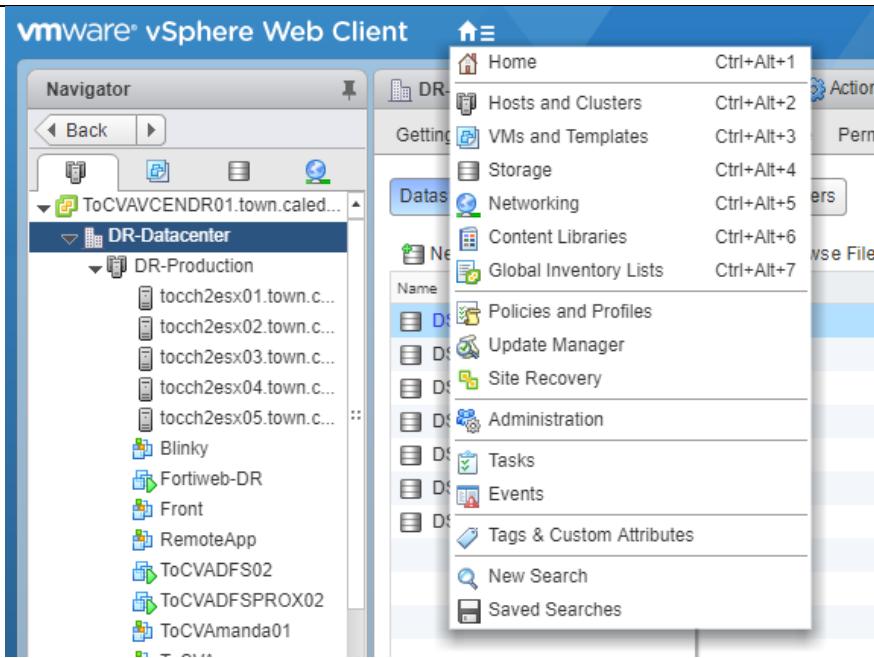
(10.10.20.11)

3. Click on vSphere Web Client (Flash)

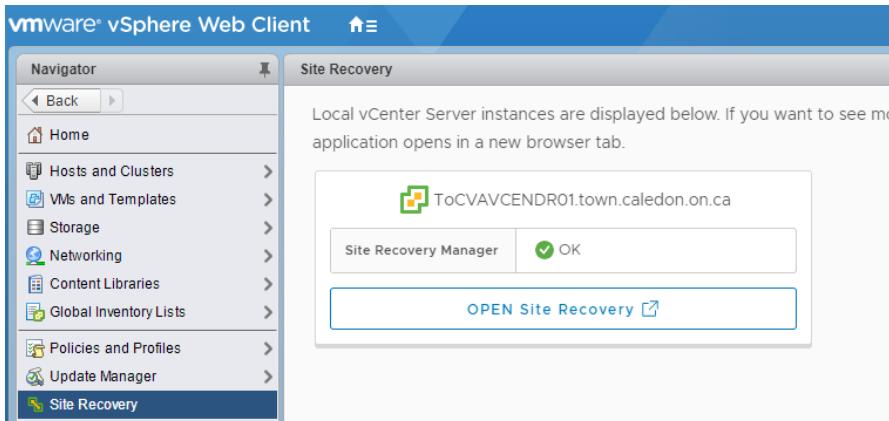
4. Login with your domain admin account



5. From the top left – click on the Home icon and select Site Recovery.



6. Click on “Open Site Recovery”. This will launch a new browser window.



7. Once the Site Recovery window opens. Click on “View Details”

The screenshot shows a web browser window titled "Site Recovery" with the URL <https://10.10.20.15/dr/#/home>. The page displays a "NEW SITE PAIR" button. Below it, there are two network icons representing site pairs: "ToCVAVCENDR01.town.caledon.on.ca" and "TOCVAVCEN01.town.caledon.on.ca". Underneath these icons, the "Site Recovery Manager" section is visible, showing "Protection Groups 2" and "Recovery Plans 2". At the bottom of the interface are "VIEW DETAILS" and "ACTIONS" buttons.

8. Enter your login information. Make sure to prefix with domain name. (Domain admin credentials)

The screenshot shows a "Log In Site" dialog box. It prompts for "Enter vCenter Server credentials". The "vCenter Server" field contains "TOCVAVCEN01.town.caledon.on.ca". The "User name" field is labeled "Enter user name" and the "Password" field is labeled "Enter password". At the bottom of the dialog are "CANCEL" and "LOG IN" buttons.

Town of Caledon Disaster Recovery Playbook – Administration Building Data Center

9. Click on the **Recovery Plans** tab and Select the associated recovery plan.

The screenshot shows a software interface for managing disaster recovery plans. At the top, there are tabs for "Site Pair", "Protection Groups", and "Recovery Plans". The "Recovery Plans" tab is selected. On the left, a sidebar lists "Recovery Plans" with two entries: "Mitel_Prod_RecoveryPlan" and "Prod_RecoveryPlan". The main area is titled "Recovery Plans" and contains a table with columns for "Name" and "Status". There are two rows in the table:

| Name | Status |
|-------------------------|--------|
| Mitel_Prod_RecoveryPlan | Ready |
| Prod_RecoveryPlan | Ready |

10. Click ... and then **Reprotect**

This screenshot shows the same software interface as the previous one, but with a noticeable difference in the "Status" column. Both "Mitel_Prod_RecoveryPlan" and "Prod_RecoveryPlan" now show "In Progress" instead of "Ready". The rest of the interface, including the sidebar and the overall layout, remains identical to the first screenshot.

11. Follow through the Wizard to enable re-protection. This will allow for failover from DR site to TownHall.

12. Once reparation steps are complete - We can click **Run** under **Recovery Plans**.

This will fail back the SRM protected VMs from DR site to Town Hall.

13. Repeat steps 9 to 12 for the other Protection group - **"Prod_ProtectionGroup"**

Important: Don't fail back '**Prod_ProtectionGroup**' until you have completed Step X (Database Fail back) in the restoration table. Initiating the fail back will power on the VMs at the Town Hall site which would require the Databases to be available first, in order for the application(s) to function.

Town of Caledon Disaster Recovery Playbook – Administration Building Data Center

| |
|---------------|
| VMs (Non-SRM) |
| |
| |
| |
| |
| |
| |