WHAT’S IN THIS GUIDE

This manual is a procedural guide that provides...

» concept overview of the data replication and failover process
» server, network and system operation requirements
» procedural steps to configure & manage data replication jobs, failovers, and related tasks
Table of Contents

INTRODUCTION OF REDUNDANT SERVER SOLUTION .................................................. 3
  WHAT HAS CHANGED SINCE V6 (IN THIS GUIDE) ................................................... 3
  TERMS & definitions USED IN THIS GUIDE ......................................................... 4
  OVERVIEW OF THE REDUNDANT SERVER SOLUTION ......................................... 5

REQUIREMENTS & SPECIFICATIONS ...................................................................... 8
  SYSTEM & OPERATIONAL REQUIREMENTS .......................................................... 8
  NETWORK SETUP REQUIREMENTS ...................................................................... 9
  SYSTEM SPECIFICATIONS FOR REDUNDANT SERVERS ...................................... 9

MAIN STAGES OF THE DISASTER RECOVERY PROCESS ......................................... 10
  OVERVIEW OF TYPICAL DISASTER RECOVERY STAGES ..................................... 10
  STAGE-1) BEFORE DISASTER ~ REPLICATION PROTECTED (SOURCE = LIVE) ......... 11
  STAGE-2) FAILURE OCCURS ~ REPLICATION DOWN (& SG Database offline) ....... 12
  STAGE-3) FAILED OVER ~ REPLICATION DOWN & TARGET GOES LIVE ............. 14
  STAGE-4) RECOVERY OPTIONS - DATA REPLICATION RESTORED .................... 15
    STAGE-4a) RECOVERED - DATA REPLICATION RESTORED (ROLES REVERSED) . 15
    STAGE-4b) RECOVERED - REPLICATION RESTORED BY UNDOING FAILOVER ....... 16

DOUBLE-TAKE “HOW TO” PROCEDURES ............................................................... 17
  HOW TO ~ ATTACH THE DVD DRIVE (WHEN NEEDED) ......................................... 18
  HOW TO ~ START THE DOUBLE-TAKE SERVICES ............................................... 19
  QUICK STEPS ...................................................................................................... 19
  HOW TO - SET UP E-MAIL NOTIFICATION FOR FAILURE ALERTS .................... 20
  QUICK STEPS ...................................................................................................... 20
  HOW TO ~ CONFIGURE THE TYPE OF FAILOVER ( manual vs. automatic ) .......... 23
  QUICK STEPS ...................................................................................................... 23
  HOW TO ~ CREATE A NEW REPLICATION JOB ................................................... 25
  HOW TO - VIEW THE ‘HEALTH’ OF A REPLICATION JOB .................................. 33
  HOW TO ~ PERFORM A ‘TEST FAILOVER’ ........................................................... 34
  STAGES OF A TEST FAILOVER ......................................................................... 34
  QUICK STEPS ...................................................................................................... 34
  HOW TO ~ IDENTIFY A REPLICATION FAILURE (MANAGE JOBS VIEW) ............. 38
  HOW TO ~ IDENTIFY A FAILURE CONDITION (MANAGE SERVERS VIEW) ........ 39
  HOW TO ~ IDENTIFY RESTORED COMMUNICATION BETWEEN SERVERS ........... 40
  HOW TO ~ PERFORM A MANUAL FAILOVER (from the Target Server) ............... 41
  HOW TO ~ REVERSE ROLES to restore data replication ................................. 44
  HOW TO ~ UNDO A FAILOVER ........................................................................ 46

SYSTEM ERRORS ................................................................................................. 47
  VIRTUAL MACHINE FAILS TO START ON TARGET WHEN FAILED-OVER ............ 47
INTRODUCTION OF REDUNDANT SERVER SOLUTION

Galaxy Control Systems offers an engineered redundant server solution using the Double-Take® Availability 7.0 data replication software on a Microsoft® Hyper-V® virtual environment. Both source and target servers are prebuilt at Galaxy Control Systems and preloaded Double-Take, Hyper-V and the System Galaxy Access Control software. See the Concept Overview section for high-level information on how the servers provide redundancy & data replication/protection.

WHAT HAS CHANGED SINCE V6 (IN THIS GUIDE)

- The System Requirements item #4 has been updated to reflect the removal of the “DT Hyper-V” service.
- All screen shots are updated to reflect the correct version of Double-Take Console using Agentless Hyper-V. Double-Take offers agent-based and agentless solutions. This guide shows the agentless solution.
- Concept Diagrams have been updated to reflect ‘the four stages of a failover and recovery
- Updated the Terms & Definitions table.
TERMS & definitions USED IN THIS GUIDE

**SOFTWARE**

| **Double-Take® Availability (DT)** | the data replication & site recovery software; manages replication between servers. |
| **Double-Take Console** | the software UI used to configure, manage, monitor the replication jobs, perform the failover, role reversal and related tasks. |
| **Hyper-V** | (VM) the Microsoft® software used to create & maintain a virtual environment; System Galaxy software & database will install and operate on the VM. |
| **System Galaxy (SG)** | the integrated access control software from Galaxy Control Systems. |

**SERVERS**

| **Source Server (live)** | the server that takes the role of “live host”; the server that is actively running the System Galaxy software on the Hyper-V environment. |
| **Target Server (standby)** | the server that takes the role of “standby server” or backup server during replication, which is storing an up-to-date image of the live host; standing by for failover/recovery. |

**PROCESS**

| **“failed”** | the activity state that indicates the Double-Take replication job has detected a failure and is no longer updating or backing-up to the standby server (replication job is not protected). |
| **Failover** | the act of performing a failover or transferring live operations to the target/standby server. |
| **“failed-over”** | the activity state that indicates that the standby server has resumed live operation; however, data is not yet being replicated/protected. |
| **healthy job status** | when the data/software is being replicated and job activity state is “Protecting”. |
| **notification** | an email that is distributed to designated addresses to notify of replication errors or warnings (optional / recommended). |
| **“protecting”** | the activity state that indicates data is being backed-up or replicated to standby server. |
| **replication** | the operation of storing the current, up-to-date copy of the data and software from a live/source server onto a standby/target server. |
| **replication failure** | a condition that interrupts the active data replication due to a fault or failure of the server hardware, system or connectivity between the live/source server and the standby/target server. |
| **reverse roles** | the operation of swapping the server roles of the target and source servers; this is done after a fail-over operation is completed. |
| **“stopped”** | the activity state showing that data replication has stopped. |
| **“synchronizing”** | the activity state showing that the Double-Take software is synchronizing the mirror image on the standby server to match the source server image. |
| **test failover** | the operation of performing a failover to test the ability of the redundant servers to correctly handle a failover process. |
| **undo failover** | the act of undoing a failover; this is typically used during system testing or when the failure reason is deemed non-catastrophic. |
OVERVIEW OF THE REDUNDANT SERVER SOLUTION

The **redundant server solution** provides a means for quick disaster recovery in case of a catastrophic failure on the live/source server. The down-time is minimized, if not completely eliminated, by the ability to switch to a stand-by server that has been mirroring the live server. This switch-over to the stand-by server is called a FAIL-OVER. There is a difference between a **failed condition** and a **failed-over condition**.

During a failure you should be aware of these things!

- During a **server failure condition**, the System Galaxy **database is offline** (i.e. not running on either server) and the **data replication is stopped/failed** (see Figure 2).

  However, all Galaxy control panels remain fully functional and do not degrade in performance because all necessary programming is stored in the panel. This means all door & lock schedules, access, credentials/cards, input & output activation, arming/disarming, relays, etc. and all hardware remains fully operational.

- Once a **Fail-Over is complete**, the System Galaxy database comes back online on the standby server, but data synchronization (mirroring) is still stopped / failed until server roles are reversed. Since SG is online, the panels will reconnect and transmit their events to the SG database. System Galaxy extended functions can resume (e.g. badging, card enrolling, monitoring, etc.). See Figure 3.

- After the failure is repaired and the downed server comes back online, the administrator can **reverse roles** and the server images will re-synchronize / replication job will resume a protected state (fig. 4).

**FIGURE 1: Redundant Servers in their Initial Roles** (live & stand-by servers are both healthy)

When the activity state of the data replication job is “protecting” and the condition is healthy, then a replica of the SG database is being updated and stored on the target/standby server. See the section on **Stages of a Disaster Recovery Process** for details about interim states such as failed, failed-over, test, and undo.
FIGURE 2: Redundant Servers are in Failure Condition (SG is not running on either server)

When a failure condition occurs at the source server, the data replication is interrupted. The state of the replication job will change from ‘protecting’ to ‘failure condition met’ and replication will “stop”. System Galaxy database will not be running on either server at this point, although the System Galaxy access control and all other hardware functions (scheduled locks/unlocks, access approval/denial, detection of hardware, arming/disarming, etc.) will all remain fully operation in a non-degraded performance.
**FIGURE 3: Target Server is Failed-Over** (SG resumes running on stand-by server/Hyper-V)

Once the FAILOVER process is performed at the target server, System Galaxy will start up (running on Hyper-V) on the standby/target server(02). Although System Galaxy is running again, redundancy or data replication has not been restored.

![Diagram showing target server failed-over](image)

**FIGURE 4: Redundant Servers have Reversed Roles** (live & stand-by servers are both healthy)

Once the failure condition is corrected/repaired, the administrator can reverse roles, meaning the target / stand-by server (02) now becomes the source; and the original source server (01) becomes the new stand-by (target) server.

When both servers are re-synchronized and the replication job is restored, the system is considered healthy again and data replication state should indicate “protecting”.

![Diagram showing roles reversed](image)
REQUIREMENTS & SPECIFICATIONS

SYSTEM & OPERATIONAL REQUIREMENTS

1. Galaxy Control Systems supports server replication using Hyper-v and Double-Take software when the redundant server solution is purchased through Galaxy.

2. Microsoft® Windows Server® 2008 R2 will be running on the host operating system of the source and target servers, as well as the virtual machines (guest image).

3. Hyper-V and Double-Take software must be installed and running on the host operating system of both the source and target servers.

4. The Double-Take services must be set to run automatically. These services must be running on the host OS of both the source and target servers:
   - Double Take (Automatic Start)
   - DT Management Service (Automatic Delayed Start)

5. The Double-Take firewall ports/exceptions must be open on both host servers and on network devices across the LAN as required (6320 TCP & UDP, 6330 TCP & UDP, 6332 TCP & UDP, and 6325 TCP & UDP).

6. You must attach the DVD drive needed to install software onto the Virtual Machine through the Settings menu in the Hyper-V Manager. However, once you have completed installing software you must detach the DVD drive from the virtual machine or it could cause a potential failure in the Failover Process.

7. The Double-Take replication job will run on the target server (standby server) and will update the data on the target server every few seconds to match the state/condition of the source server (live server).

8. Double-Take should be configured to send email notifications for warnings and errors when a replication failure occurs. This is especially recommended for servers using manual failover procedures.

9. The failover process may be initiated when a replication failure occurs.

   **IMPORTANT:** The cause of a replication failure should be carefully evaluated in order to determine whether performing a failover is the best course of action. Once a failover has been deemed necessary, the process must be completed and the failure resolved before data replication can be re-established.

   **IMPORTANT:** the servers must be re-synchronized and roles reversed before server redundancy is restored.

10. When roles are reversed, Server-B becomes the source and Server-A becomes the target/standby server. The names of the servers will not change or swap, only their roles.

11. It is possible to undo a failover, in which case the server roles are not reversed; but the target server is rolled-back and resumes its role as the standby server and the job of data replication.

   **CAUTION:** It is possible to experience data loss if any activity, such as card editing, has occurred on the server after a failover is completed and the server became live. Any changes occurring after going live would be rolled-back and therefore lost.
NETWORK SETUP REQUIREMENTS

1. You need three (3) static IP Addresses. One for each server and one for the Virtual Machine. Assign IP addresses to 2nd NIC card on each host server.
2. IP Addresses must be valid within the Network IP Range for each server.
3. It is recommended the System Administrator tags or labels the source server at all times.

SYSTEM SPECIFICATIONS FOR REDUNDANT SERVERS

In the Galaxy redundant server implementation, the following infrastructure will be observed:

HOST OS: SERVER-A and SERVER-B

- Both servers (A/B) will run Microsoft Server 2008 R2 as the host operating system.
- Both servers (A/B) will run the Double-Take services set to start automatically: Double Take, DT Hyper V, DT Management.
- Both servers (A/B) will open both TCP & UDP ports 6320, 6330, 6332, and 6325 (necessary for Double-Take).
- Both servers (A/B) will have the Double-Take Console software installed and able to run when in the role of the standby/target.

GUEST OS:

- The Hyper-V guest virtual environment will run Microsoft Server 2008 R2 as the operating system.

SERVER ROLES and RESPONSIBILITIES

- The server operating in the live role (source) will run System Galaxy, database and services on its guest virtual environment.
- The server operating in the standby role (target) will run the Double-Take Console to monitor and maintain data replication.
- The standby/source server will support card editing and event monitoring of the System Galaxy software.
- The standby/target server will perform failover in the event of a catastrophic failure of the live server.
- Once a failover is completed the servers will reverse roles and re-synchronize before resuming data replication.

FIGURE 5: CONCEPT OF A HEALTHY REDUNDANT SERVER ENVIRONMENT

REDUNDANT SERVERS - PROTECTED STATE

Live Operation
( primary/source )

SERVER A

- Host OS = SVR 2008 R2
- Double Take Software & Console
- Double Take Services

GUEST VIRTUAL MACHINE
Guest OS = SVR 2008 R2

System Galaxy
Event Monitoring / Card Editing
SG System Galaxy DB, Software and GCS Services
LAN Connection IP = XXXXXX.XXX
{ Guest Virtual NIC }

“Protecting” Back-up Operation
( standby/target )

SERVER B

- Host OS = SVR 2008 R2
- Double Take Software & Console
- Double Take Services

HYPER-V VIRTUAL MACHINE
Guest OS = SVR 2008 R2

DATA REPLICATION

HYPER-V VIRTUAL MACHINE
Guest OS = SVR 2008 R2

A concurrent copy of System Galaxy software & database is being stored here

LAN Connection 1
Virtual Switch
IP = XXX.XXX.XXX
{ NIC-2 }

DATA REPLICATION NETWORK

DATA REPLICATION CONNECTION*

ETHERNET LAN CONNECTION 192.68

Switch

TO GALAXY ACCESS CONTROL PANEL B

* Data replication (NIC-2) can use an Ethernet cable to same or different switch as NIC-1; or direct crossover cable.
MAIN STAGES OF THE DISASTER RECOVERY PROCESS

This section provides a basis for preparing a disaster recovery plan. It identifies the main stages of the disaster recovery process.

The tables and diagrams in this section show when data replication is ‘protecting’ and which server is in the active (live) role throughout the failure and recovery.

OVERVIEW OF TYPICAL DISASTER RECOVERY STAGES

When a failure occurs that is deemed worthy of a failover and recovery, you will follow the path described in the table below.

TYPICAL DISASTER RECOVERY STAGES - SERVERS REVERSE ROLES:

<table>
<thead>
<tr>
<th>RECOVERY STAGES</th>
<th>STATE OF REPLICATION</th>
<th>SERVER-A</th>
<th>SERVER-B</th>
</tr>
</thead>
<tbody>
<tr>
<td>1) BEFORE DISASTER</td>
<td>PROTECTING (HEALTHY)</td>
<td>SOURCE = LIVE</td>
<td>TARGET = STANDBY</td>
</tr>
<tr>
<td>2) FAILURE OCCURS</td>
<td>DOWN/UNKNOWN</td>
<td>(?)</td>
<td>TARGET = STANDBY</td>
</tr>
<tr>
<td>3) FAILOVER</td>
<td>DOWN</td>
<td>DOWN</td>
<td>TARGET = LIVE</td>
</tr>
<tr>
<td>4A) RECOVERED ~</td>
<td>PROTECTING (HEALTHY)</td>
<td>TARGET = STANDBY</td>
<td>SOURCE = LIVE</td>
</tr>
<tr>
<td>REVERSE ROLES</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4B) RECOVERED ~</td>
<td>PROTECTING (HEALTHY)</td>
<td>SOURCE = LIVE</td>
<td>TARGET = STANDBY</td>
</tr>
<tr>
<td>UNDO FAILOVER*</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*WARNING: be aware that undoing a failover can cause data loss of any activity, system programming or card editing that takes place while the system is failed-over (stage-3) and data replication is down.
STAGE-1) BEFORE DISASTER ~ REPLICATION PROTECTED (SOURCE = LIVE)

In the diagram below, the system is operating normally and disaster has not occurred:

- Server-A is the live/source and Server-B is the standby/target.
- The diagram shows System Galaxy is running live/operating normally on the source server.
- Data Replication is occurring. The condition of the replication job in the Double-Take Console will show that the ACTIVITY is “Protecting” and DATA STATE is “OK”.

FIGURE 6: CONCEPT OF DATA REPLICATION IN PROTECTED STATE (STAGE-1 HEALTHY)
STAGE-2) FAILURE OCCURS ~ REPLICATION DOWN (& SG DATABASE OFFLINE)

When a failure occurs that interrupts data replication, there are many possible causes. This section does not cite every possible reason for a replication failure; however it presents a few common causes to provide examples to understand the need to plan for several disaster recovery responses.

It is important to understand why the failure occurs and what effect it has on live operation and actively protected data replication. Some failures interrupt replication but do not require a failover since live operation is not interrupted. Correcting such a failure and re-synchronizing the replication job will restore the replication. Other failures could require a failover to be performed in order to restore live operation of the access control system. In those cases data replication will be restored when the failure is corrected and the job is restarted. See the table below for tips.

### IMPORTANT:
Galaxy hardware (control panel) remains fully functional during server/database communication interruptions. Access control, schedules, arming/disarming, door lock/unlock, input/output operation remains in tact when the server/database are offline. Event logging is saved to a buffer in the panel and retransmitted to the database when the database is online/restored and panels can reconnect to the server.

### SOME CAUSES FOR REPLICATION FAILURE:

<table>
<thead>
<tr>
<th>CAUSE OF INTERRUPTION</th>
<th>DURATION</th>
<th>SERVER AFFECTED</th>
</tr>
</thead>
<tbody>
<tr>
<td>1) planned outage (e.g. reboot for OS updates)</td>
<td>brief outage performed under controlled conditions</td>
<td><strong>Live source is down – replication down</strong>&lt;br&gt;In this case a failover is not warranted. Resynch the replication job.</td>
</tr>
<tr>
<td>2) unplanned outage (e.g. power interrupt)</td>
<td>unexpected outage that is identified as brief or acceptable</td>
<td><strong>one or both servers down – replication down</strong>&lt;br&gt;In this case a failover may not be necessary if the outage is brief enough. Resynch job ASAP.</td>
</tr>
<tr>
<td>3) network connectivity is interrupted between SG panels and live server</td>
<td>unexpected interrupt that requires resolution</td>
<td><strong>Replication is not affected – restore connectivity to panels. Offline events are available via SG reports after panel buffer is retransmitted.</strong></td>
</tr>
<tr>
<td>4) network interrupt between the two redundant servers</td>
<td>unexpected interrupt that requires resolution</td>
<td><strong>Replication down – resolve &amp; restore connectivity.</strong> Resynch job ASAP.</td>
</tr>
<tr>
<td>6) catastrophic failure of standby/target server</td>
<td>unexpected outage</td>
<td><strong>Target server down – replication job is dropped.</strong>&lt;br&gt;In this case a failover is not possible. Restore the standby server and restart ASAP.</td>
</tr>
<tr>
<td>7) catastrophic failure of live source server</td>
<td>unexpected long-term outage</td>
<td><strong>Source server is down – replication down. Failover is warranted to continue/resume live operation</strong> on the target/standby server. Restore the down server and restart replication job ASAP.</td>
</tr>
</tbody>
</table>
FIGURE 7: CONCEPT OF DATA REPLICATION IN FAILED/STOPPED STATE (STAGE-2 FAILED)

In this stage, the Live server is down, replication has stopped/failed and System Galaxy database is offline.

The standby server has the last/latest copy of the live image and is ready to for the failover process to begin. Galaxy panels are fully operational and will reconnect to the database when it comes online from the standby server. In order to bring the standby image online, you must failover the target server.

The SG access control panels continue operating at full capacity and will log their events to an internal buffer until they can reconnect to the database and transmit their buffered events. Each panel’s buffer limit is 10,000 events. When the limit is reached the panel continues logging current events to its buffer but the oldest events are dropped. Therefore, it is imperative that the database is brought back online as soon as possible.
STAGE-3) FAILED OVER ~ REPLICATION DOWN & TARGET GOES LIVE

In the diagram below, a catastrophic failure has occurred at Server-A; Server-B has completed the failover process.

Notice: A failover can be performed manually or automatically. A manual failover process is recommended to give a system administrator a chance to determine whether a failover is the best course of action. Some causes of replication failure may not interrupt live operation of System Galaxy on the source server. Likewise, the down time of a known outage might be so brief that it is acceptable in comparison to the time/intensity of failing-over to the standby server. If normal operation can continue on the source server during the repair, then a failover may not be necessary, thus replication can resume when the outage is resolved.

Once the failover has occurred the following is true:

» Server-A is no longer operating as the live/source.

» Server-B is still the standby/target server, and System Galaxy is now operating live on the standby server.

» Data Replication is not occurring and there is no redundancy/protection.

IMPORTANT: If Server-B should go down during the failed-over/unprotected state, functions supported in the System Galaxy software (such as event monitoring, operator commands, and card editing) will not be available.

IMPORTANT: System Galaxy’s access control is designed to continue functioning in a non-degraded mode and without interruption even when the System Galaxy software or communication/event servers are offline. Access control is based on programming of cards, schedules & access rules that are stored at the access control panel.

FIGURE 8: CONCEPT OF DATA REPLICATION IN FAILED-OVER STATE (STAGE-3 FAILED-OVER)
STAGE-4) RECOVERY OPTIONS - DATA REPLICAATION RESTORED

Once the failure is resolved and Server-A is restored, there are two possible options.

1. The server roles can be reversed (4a): makes SERVER-A the new standby server and SERVER-B the source.

2. The failover can be undone (4b) instead of reversing roles.

   **WARNING: UNDOING A FAILOVER IS NOT RECOMMENDED** for reasons other than a “TEST FAILOVER”. DATA LOSS can occur if any time/data transfer has elapsed during the downed server.

STAGE-4a) RECOVERED - DATA REPLICAATION RESTORED (ROLES REVERSED)

Once the failure is resolved and Server-A is restored, the server roles can be reversed.

» Server-B becomes the live/source; and System Galaxy continues running normally on the guest OS of Server-B.

» Server-A becomes the standby/target.

» Data Replication resumes on Server-A. After re-synchronization is completed, the state of the replication job in the Double-Take Console will show ACTIVITY is “protecting” and DATA STATE is “OK”.

   **NOTE:** The servers must be re-synchronized before data replication is restored and is once again protected.

FIGURE 9: CONCEPT OF ROLES REVERSED & RESUME PROTECTED STATE (STAGE-4 PROTECTED)

---

*Data replication (NIC-2) can use an Ethernet cable to same or different switch as NIC-1; or direct crossover cable.*
Once the failure is resolved and the source server is restored, the failover can be undone**.

» Server-A is restored to run as live/source again; System Galaxy returns to running on the guest OS of Server-A.
» Server-B becomes the standby/target again.
» Data Replication resumes on Server-B. After re-synchronization is completed, the state of the replication job in the Double-Take Console will show ACTIVITY is “protecting” and DATA STATE is “OK”.

**WARNING: be aware that undoing a failover can cause data loss of any activity, system programming or card editing that takes place while the system is failed over (stage-3) and data replication is down. Undoing a failover has the same effect on System Galaxy as ‘rolling back’ to an earlier database. Undoing a failover is typically used when a test failover is performed. During the test, you can prohibit use of the access control software to prevent data loss.
DOUBLE-TAKE “HOW TO” PROCEDURES

This section contains the step-by-step instructions for the main tasks involved with configuring and operating the Double-Take server.

SETUP AND CONFIGURATION:

- HOW TO – Attach a DVD Drive (when needed)
- HOW TO – Start the Double-Take services (both target and source servers)
- HOW TO – Set Up E-mail Notification for Failure Alerts
- HOW TO – Configure the Type of Failover

MANAGING DATA REPLICATION

- HOW TO – Create a New Replication Job
- HOW TO – View the Health of a Replication Job
- HOW TO – Perform a TEST Failover & Recover Data Replication
- HOW TO – Identify a Replication Failure (Manage Jobs View)
- HOW TO – Identify a Failure Condition (Manage Servers View)
- HOW TO – Identify communication is restored between servers.
- HOW TO – Perform a Manual Failover from the Target Server
- HOW TO – Reverse Roles to Restore Data Replication
- HOW TO – Undo a Failover

SYSTEM ERRORS

- Virtual Machine fails to start on Target Server when Failed-over
1. Go to the server’s host operating system and double-click the Hyper-V Manager startup icon on the desktop to open Hyper-V Manager.

![Hyper-V Manager](image)

2. Right-click the SGSERVER guest name appearing in the Virtual Machines list, and select the Settings menu option.

![Virtual Machines](image)

3. In the hardware tree, select the DVD Drive option and specify the Media by choosing the Physical DVD Drive option and selecting the drive name from the droplist.

**IMPORTANT:** detach the DVD drive when not in use. If you leave a DVD drive attached and a failure occurs, it could interfere with the failover process.
HOW TO ~ START THE DOUBLE-TAKE SERVICES

IMPORTANT
- Double-Take services must be running at both servers (source and target).
- Services must be started before any configuration or operation can occur.

QUICK STEPS

1. Open the Services window at each server:
   - START > Control Panel > Administrative Tools > Services.
2. Locate the two Double-Take services. Ensure Status is “started” and Startup Type is “automatic”.
   - Double-Take
   - Double-Take Management
3. To start each service, right-click on the service name and select ‘START’ from the shortcut menu.
4. To set services to start automatically, right-click on the service name and select ‘PROPERTIES’ from the shortcut menu. In the property screen, select “automatic” in the Start-up Type droplist.
HOW TO - SET UP E-MAIL NOTIFICATION FOR FAILURE ALERTS

IMPORTANT

- Double-Take services must be running at both servers (source / target).
- You must configure E-mail Notification at both servers (source and target).

QUICK STEPS

1. Go to the Target Server's host OS and double-click the [Double-Take Console] desktop icon to open the Double-Take Console software.

2. From the console toolbar, click on the [MANAGE SERVERS] button.

3. Right-click the desired server name and select ‘View Server Details’ in the shortcut menu.
4. Click the ‘Edit server properties’ link in the TASKS list on the right side the screen.

![Server Properties](image1)

5. Expand the E-mail Notification option in the Server Properties screen.

![E-mail Notification](image2)
6. Check the [Enable Notification] option and enter the Mail Server Address (mailserver.domain.com).

7. Check the [Log onto email server] option and enter the Login Credentials for the e-mail server.

8. Enter the From Address, and Send To address (yourname@domain.com).

9. Enter the desired text in the Subject Prefix field.

10. (optional) You do not need to enable the add event description option – this will make your subject line longer and you will see this in the message content anyway.

11. Check the [Warning] and [Error] options.

12. Click [TEST] to verify your e-mail will work with these settings.

13. Save your settings and repeat these steps for the other Server.
HOW TO ~ CONFIGURE THE TYPE OF FAILOVER ( manual vs. automatic )

You must determine whether you want to depend on a manual failover process or an automatic failover process. A manual failover/cutover must be performed by the system administrator after Double-Take software has reported that a ‘condition for failure’ has been met. An automatic failover is initiated by the software whenever the system has met a ‘condition for failure’.

IMPORTANT
- If using a manual failover, the user must perform the failover from the TARGET SERVER.
- An automatic failover will cut-over replication to the target server without user intervention.

QUICK STEPS

The type of failover is configured in the Job Properties screen. This can be done from either the target or the source server once the job has been created.

1. Click the [MANAGE JOBS] button on the main toolbar, then click the [VIEW JOB DETAIL] button on the lower toolbar.

2. Click the EDIT JOB PROPERTIES link under the TASKS list, on the right side of the screen.
3. In the *Edit Job Properties* page, expand the **Failover Monitor section** and set the following:
   
   b. (Recommended) choose [Total Time to Failure] option and set Time to the desired value.
   c. Set the [monitor on this interval] value to an appropriate value.
   d. Enable (“check”) the [Wait for User to Initiate Failover] option if you want the system to wait for the administrator to **manually** initiate a failover/cutover. *Unchecking this option will allow the system to automatically failover when a condition for failure is met.*

   ![Double-Take Console](image)

   **The “Wait for User to Initiate” option:** Enabling (checking) this option means the system administrator must manually initiate a failover when the software reports that a ‘condition for failure’ has been met (e.g. Target server looses communication to the Source server).

   Disabling (unchecking) this option means the Double-Take system automatically initiates a fail-over when any ‘condition for failure’ has been detected by the software. *An automatic failover may be undesirable in controlled tests/planned outages (e.g. server/router reboot).*
HOW TO ~ CREATE A NEW REPLICATION JOB

The steps below show how to create a new replication job in the exception case that the target server goes down and the job is dropped.

1. Go to the target server’s host operating system and double-click the Double-Take Console startup icon on the desktop to open DT Console.

2. Click the 🌟 GET STARTED button (on the main toolbar) to open the task screen; and then double-click on the ‘Double-Take Availability’ task.
3. Double-click the ‘Protect files and folders, application or entire server’ task.

4. Under the CONNECTED SERVERS list, select or highlight the name of the Virtual Machine (or the source server) that needs to be protected. Click the NEXT button to continue.
5. Under SERVER WORKLOADS, choose the data you want to protect.
   a. In the Workload Types list-view, select/highlight the “Agentless HYPER-V”
   b. In the Workload Items list-view, [+] click the button to expand “Hyper-V Machine”
   c. Then [check] enable the name of the Hyper-V Session (i.e. “Server”) to be protected
   d. Click NEXT to continue.
6. Highlight or select the name of the target server in the list of CURRENT SERVERS. Click NEXT to continue. This will be the standby server.

7. Expand Failover Monitor. Set the Protection Options as appropriate: Enable or “check” [Monitor for Failover] option. Also enable the [Wait for User to Initiate] option. Click NEXT to continue.
8. Expand the “Replica Virtual Machine Location” options. Choose the location on the target server that will store the replica of the virtual machine. The full path must be selected. Click NEXT to continue.

**IMPORTANT:** Make sure you observe the minimum space requirement.
   a. Enter a user defined name for the virtual machine replica (or accept the default if suitable).
   b. Choose the Target Network Adapter.
   c. If using a V-LAN, set the Target V-LAN ID.
   d. Click NEXT to continue
10. Expand the NETWORK ROUTE option.
   a. Choose the IP address of the network route.
   b. Click the Click NEXT to continue.
11. Visually verify options are set as required. If there is a RED-X or (!), you must correct the indicated problem. Click RECHECK. When all CheckList Items are OK, click FINISH to continue.

12. The user is returned to the MANAGE JOBS screen and the replication will connect and begin synchronizing with the source/virtual machine. Synchronizing may take a while. Eventually the job Status should complete and display “Protecting” in the Activity column.
HOW TO - VIEW THE ‘HEALTH’ OF A REPLICATION JOB

1. Go to the Target Server's host OS: Double-click the Double-Take Console desktop icon to open Double-Take Console.

2. Click the MANAGE JOBS button on the main toolbar.

3. List of Jobs Panel: When data is actively replicating, the Job status indicates a green arrow and the Activity column displays “Protecting”.

4. Job Highlights Panel: The Target Data State should indicate “OK”
**HOW TO ~ PERFORM A ‘TEST FAILOVER’**

THIS SECTION SHOWS YOU HOW TO INITIATE A TEST FAILOVER AND RECOVER DATA REPLICAION.

A test failover tests the ability of your system to failover (or cutover) when a ‘condition for failure’ is met. You do not have to induce an actual failure in order to perform a test failover. The option to perform a failover as a test is always available.

**STAGES OF A TEST FAILOVER**

The tables below describe the failover/cutover sequence. The failover sequence is the same for manual and automatic failovers/cutovers.

<table>
<thead>
<tr>
<th>RECOVERY STAGES</th>
<th>STATE OF REPLICAION</th>
<th>SERVER- 01 (A)</th>
<th>SERVER- 02 (B)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1) Before Cutover</td>
<td>PROTECTING/HEALTHY</td>
<td>SOURCE = LIVE</td>
<td>TARGET = STANDBY</td>
</tr>
<tr>
<td>2) Failure condition met *</td>
<td>STOPPED</td>
<td>SOURCE = FAILED</td>
<td>TARGET = STANDBY</td>
</tr>
<tr>
<td>3) FAILOVER</td>
<td>FAILED OVER</td>
<td>SOURCE = STOPPED</td>
<td>TARGET = LIVE</td>
</tr>
<tr>
<td>4) UNDO FAILOVER</td>
<td>SYNCHRONIZING</td>
<td>SOURCE = LIVE</td>
<td>TARGET = STANDBY</td>
</tr>
<tr>
<td>5) After Recovery</td>
<td>PROTECTING/HEALTHY</td>
<td>SOURCE = LIVE</td>
<td>TARGET = STANDBY</td>
</tr>
</tbody>
</table>

**IMPORTANT**

- Double-Take services and software must be running on both servers (source and target).
- Hyper-V must be properly configured and running on both servers.
- The Galaxy virtual session will run on the same server that is performing the job replication.
- Galaxy hardware (control panel) remains fully functional during failover tests.
- Initiate a failover from the target machine.
- **DOING A TEST FAILOVER WILL TEMPORARILY INTERRUPT THE DATA REPLICAION.** You must UNDO FAILOVER to resynchronize & restore data replication.

**QUICK STEPS**

1. Go to the **Target Server’s** host OS and double-click the [Double-Take Console] desktop icon to open the Double-Take Console software.
2. Click the **MANAGE JOBS** button on the main toolbar.

3. On the Jobs toolbar, click the [FAILOVER](#) button (yellow arrow over a blue dot).

4. Select the option to ‘**Perform test failover**’ and click [Failover] button.
5. Job status will change to “FAILING OVER: CONFIGURING TARGET”.

![Job status changing](image)

6. Job status will change to “FAILED OVER” when complete.

![Job status status](image)

**IMPORTANT:** During a TEST FAILOVER, the replication is no longer occurring and, unlike a real failover, the target virtual machine does not assume the role of hosting the System Galaxy software. System Galaxy remains live on the source virtual machine.
7. Select the UNDO FAILOVER button to restore the server redundancy. *Double-Take will begin undoing failover and powering-off the target virtual machine.* (Remember System Galaxy has remained live on the source virtual machine – therefore no interruption of SG is incurred.)

8. The replication job will undo failover and begin “synchronizing” (shown below) the source and target server and replication will resume.

9. The activity should return to “protecting” and the data status = “OK” / “HEALTHY”.
HOW TO ~ IDENTIFY A REPLICATION FAILURE (MANAGE JOBS VIEW)

A replication failure at the source server will interrupt the source server’s ability to continue protecting the system. The failure will be reported through emails and status changes. You will go to the Target Server to confirm the failure.

1. Go to the Target Server’s host operating system and double-click the Double-Take Console startup icon on the desktop to open DT Console.

2. Click the MANAGE JOBS button.
   a. The replication job may display a Red-X (it depends on the reason for failure)
   b. You should get email(s) for a failure if you are properly set up to receive notifications.
   c. Job Highlights panel may also show a red-X or caution symbol indicating the failure.
   d. The FAILOVER button will be enabled/ON at the target server.
   e. When a failure condition occurs, you will not be able to View Server Events for the source server. However you may still be able to see Job Logs both the target and source server during a failure condition.
HOW TO ~ IDENTIFY A FAILURE CONDITION (MANAGE SERVERS VIEW)

When failover of the Target Server is complete, the failure condition at the Source Server must be corrected in order to restore the replication process.

While the source server is in the failed condition it may (or may not) indicate a RED-X for the server status indicator in the Manage Servers list-view.

1. Click the MANAGE SERVERS button on the Target Server.

2. You may notice that the source server is toggling between “Idle” and “Authenticating”, as the Double-Take software attempts to connect to the source server.

3. The Double-Take software should display a status message at the bottom of its window status bar “(!) Jobs with warnings #” or “(X) Jobs with errors #” when a failure condition exists.

Target Server attempting to connect during a failure condition at the Source Server

NOTE: From the target server, open Double-Take Console and click Manage Servers button to view the state of the failed server. During a failover/failure, the target server may still be able to see job logs for both servers, but will probably not be able to view the ’server events log’ for the source server.
HOW TO ~ IDENTIFY RESTORED COMMUNICATION BETWEEN SERVERS

Once the source server is restored/repaired or the reason for the loss of communication is corrected, the source server will appear in the list of servers with a yellow key (see image below).

1. Click the MANAGE SERVERS button on the Target Server.

2. Both the source and target servers will show ACTIVITY status of “Idle”, when the Double-Take software successfully connects to the source server.

3. The Double-Take software should display a status message at the bottom of its window status bar “(!) Jobs with warnings #” or “(X) Jobs with errors #” when a failure condition exists. The Job Warning and Job Error status will still display at the bottom of the screen until job is restored.

Target Server connected & failure condition at the Source Server corrected
HOW TO ~ PERFORM A MANUAL FAILOVER (from the Target Server)

NOTICE: In case of a complete hardware failure on the source server, contact Galaxy technical support. Return the failed server to Galaxy to be repaired / rebuilt.

NOTICE: In the case of other failures, you will restore your network connection as soon as possible

NOTICE: Once the failover is complete on the TARGET machine, all System Galaxy updates/changes will start being committed to the Target server Virtual Machine – System Galaxy will resume normal operation.

1. Go to the **Target Server's** host operating system and double-click the **Double-Take Console** startup icon on the desktop to open DT Console.

   ![Double-Take Console](image)

2. Click the **MANAGE JOBS** button.

3. On the Jobs toolbar, click the **FAILOVER** button (yellow arrow over a blue dot).

   ![Manage Jobs](image)

4. When the Failover dialog opens, choose Failover Live Data option and click **FAILOVER** button.

   ![Failover and Cutover](image)
5. The Double-Take Job ACTIVITY status will change to ‘Failing Over’

6. The Double-Take Job ACTIVITY status will change to ‘Failed Over’ when the failover process completes.

**IMPORTANT:** System Galaxy hardware will continue to be fully operational during the failover. The System Galaxy software is fully operational on the Target server’s Hyper-V session – see step 7 on the next page.

During a failover, the data replication is interrupted and redundancy is not ensured. After you have repaired or corrected the failure condition, you must decide whether to reverse rolls or undo the failover in order to restore redundancy and data replication. Data replication will be restored once you reverse rolls or undo failover.
7. Verify the system is running by opening the Hyper-V Manager at the Target Server. Go to the target server’s host operating system and double-click the Hyper-V Manager startup icon on the desktop to open Hyper-V.

8. The Hyper-V Manager on the TARGET machine will show the VM status ‘Running’

**NOTE:** System Galaxy hardware will continue to be fully operational during the failover. System Galaxy panels are designed to continue providing access control and remain fully functional (according to their programming) even if the System Galaxy database is offline. Events are buffered in the panel’s memory until connectivity is restored.
HOW TO ~ REVERSE ROLES to restore data replication

Once the source server connection is restored, you must determine whether to **Reverse Roles** of the target and source servers; or **Undo the Failover**, which could risk data loss.

**REVERSE ROLES** – Reversing roles will swap the role of the target (standby) and source (live) servers. If you have completed a failover, then your target machine is currently supporting the live operation of System Galaxy. Once the failure is corrected/repaired, you must reverse roles in order to restore redundancy. The original source server will become the standby/target server and the target will become the source.

**UNDO FAILOVER** – *this option is only recommended for a TEST FAILOVER.*

---

**CAUTION for Data Loss:** If you choose to **Undo Failover**, you will lose any/all updates and changes that have occurred on the **TARGET** server’s Virtual Machine since the initiation of the failover. When a real-time failover occurs, the target server takes over the live support of the System Galaxy operational updates - all changes will be lost if you undo failover.

**IMPORTANT:** When you reverse roles, you will cause the target server to become the source server; and the source server will become the target. Update your labels and documentation.

1. Click **MANAGE JOBS** from the Target Server toolbar.

2. Click the **REVERSE ROLES** button – note the Job ACTIVITY status is showing “Reversing”. 

---

![Manage Jobs Interface](image)
3. Click YES to proceed.

4. The job ACTIVITY status will change to ‘Connecting...’ and then ‘Synchronizing (##%)’. You will see that the standby server will become the source server and mirroring and replication will resume.

5. Once synchronization is completed, the ACTIVITY state returns to PROTECTING and server redundancy is established. Also no job errors or warnings should display.
HOW TO ~ UNDO A FAILOVER

Undoing a failover is typically only recommended for undoing a TEST FAILOVER. You would not attempt to undo a failover if a failure condition has not been corrected.

**CAUTION: DATA LOSS IS POSSIBLE - If you choose to Undo Failover, you will loose any/all changes that have occurred on the TARGET server’s Virtual Machine since the completion of the failover.**

1. From the tool bar, choose UNDO FAILOVER button (Yellow arrow with a red-x) – the ACTIVITY column should change from FAILED OVER to POWERING DOWN.

2. The ACTIVITY should change to ‘Synchronizing (%)’ and Mirroring should change to ‘In progress’.
SYSTEM ERRORS

VIRTUAL MACHINE FAILS TO START ON TARGET WHEN FAILED-OVER

One reason the virtual machine could fail to start when trying to initiate failover on the target machine is that the DVD drive used to install software is still attached to the virtual machine.

SYMPTOM:

UNABLE TO START THE VM: STATE is OFF / Fail to Start with attachment error.

In Hyper-V Manager, you will notice that the Server ‘STATE’ is OFF and when you try to start the Virtual Machine. When the VM attempts to start, it will return a critical error stating the VM failed to start due to an ATTACHMENT – Error: The system cannot find the file specified – see images below.
PROBLEM: Cause

UNABLE TO START THE VM: DVD is still attached to the Virtual Machine.

Open the server settings and set the DVD Drive to NONE OPTION

IMPORTANT: ALWAYS *detach* the drive when not in use by choosing NONE to prevent failover failure.