

# QHP803

## BUSINESS CONTINUITY PLAN - IT (Disaster Recovery Plan)

## Table of Contents

1. INTRODUCTION .....	4
2. SCOPE .....	4
3. PURPOSE .....	4
4. OBJECTIVES.....	4
5. ROLES AND RESPONSIBILITIES .....	5
.6 REQUIRED RESOURCES .....	5
7. PRIMARY, SECONDARY, AND BACKUP LOCATIONS .....	6
8. INTERESTED PARTIES .....	8
9. AUTHORITY TO ACTIVATE .....	9
10. CRITERIA FOR ACTIVATING .....	9
11. PLAN ACTIVATION AND IMMEDIATE RESPONSE PROCEDURE .....	9
12. PRIORITIZED ACTIVITIES.....	10
13. IMPACT OF DISRUPTION ON PRIORITIZED ACTIVITIES OVER PREDETERMINED TIMEFRAME.....	10
.14 RESUMPTION OF PRIORITIZED ACTIVITIES .....	10
.15 RETURN TO BUSINESS AS USUAL .....	10
16. Testing.....	11
17. DOCUMENTATION AND RECORDS .....	11
.18 RELEVANT LEGISLATION .....	11
19. RELATED POLICIES AND FORMS .....	11
20. FEEDBACK.....	12
21. DOCUMENT CONTROL AND OWNERSHIP.....	12
APPENDIX A - Avaya IP Telephony (IPT) Phone System .....	13
PROCEDURE – Avaya Phone Failover .....	15
PROCEDURE – Avaya Phone Failback.....	17
APPENDIX B – Turning Data Centres Off/On .....	19
PROCEDURE - Switching 'OFF' the Aldar Data Center.....	19
PROCEDURE - Switching 'ON' the Aldar Data Centre.....	22
PROCEDURE - Switching 'OFF' the Warehouse Data Center.....	24
PROCEDURE - Switching 'ON' the Warehouse Data Centre.....	26
APPENDIX C – Data Recovery .....	27
PROCEDURE - VM Recovery .....	28

PROCEDURE - Guest OS File or Data file Recovery .....	33
PROCEDURE - Planned Failover .....	37
<b>APPENDIX D – Network failover- public services.....</b>	<b>42</b>
PROCEDURE – Activating the Public Services in network Failover.....	42

## 1. INTRODUCTION

As an emergency pre-hospital medical services provider, the continuous availability of National Ambulance's services is critical to the community and stakeholders. Potential disruptions need to be identified at the earliest opportunity in order to respond efficiently and in a timely manner. This Business Continuity Plan for IT addresses all aspects of the organization's response from the detection of an incident through to returning to 'business as usual', including communication during the disruption between all participants.

Managing and responding to disruptions that may impact National Ambulance's operations is addressed in this Business Continuity Plan in alignment with NCEMA 7000:2021 Standard. This will ensure the delivery of prioritized activities within the predetermined timelines in the event of disruptions.

This plan is relevant to the Risk Evaluation and Management System Component.

## 2. SCOPE

The scope of this plan applies to Information Technology (IT) and all supporting functions required to deliver these operations including ACC, Operations, and other departments.

This plan includes the main steps required to trigger, implement, and recover back from IT Disaster Recovery (DR) for National Ambulance Head Office services.

It does not include disaster recovery plans for service providers other than where connections to those service providers enters the National Ambulance Head Office.

## 3. PURPOSE

The purpose of this BC Plan is to provide the information that the response team requires and the actions they need to take in order to ensure effective and timely response to disruptions. This Plan shall set the requirements needed for detecting potential incidents and responding to disruptions in order to shorten their duration, limit their impact, and protect those affected.

In addition, this plan addresses the risks identified in National Ambulance's (NA's) business continuity risk assessment relating to IT Operations and set out specific procedures to address disruptions or emergencies related to IT critical operations.

## 4. OBJECTIVES

The objectives of this BC Plan are to:

- Provide an overview of how IT will respond to a disruptive incident affecting its business continuity
- Set out how IT business continuity plans will be invoked
- Define how decisions will be taken with regard to responding to an incident
- Explain how communication within National Ambulance and with external parties will be handled
- Provide contact details for key people and external parties

## 5. ROLES AND RESPONSIBILITIES

Designation	Roles and Responsibilities	Contact Details
IT BC Plan owner	Ensure all IT DR (BC) plans and procedures are current and tested	– <b>IT Manager</b> (TBC, delegate: IT Team Leader Sachien Dalvi 0563054162)
NA Executives	Approve IT BC procedure to be triggered	– <b>CEO</b> (Ahmed Al Hajeri) – <b>CAMO</b> (Dr Ayman Ahmad) – <b>CFO</b> (Charles Arnestad)
NA Directors ACC Manager	<ul style="list-style-type: none"> <li>– Act cooperatively with another member from this group to trigger the DR Plan</li> <li>– Mobilizing DR Team once triggered</li> <li>– Inform Executive that DR Plan has been activated</li> </ul>	<ul style="list-style-type: none"> <li>– <b>ACC Manager</b> (Waseem Khan, 050 736 1791)</li> <li>– <b>Operations Director</b> (Dr Firas Al Kurdi, 050 720 6633)</li> </ul>
IT Manager QHSE & BC Manager ACC Manager	<ul style="list-style-type: none"> <li>– Mobilizing DR Team on receipt of a DR Trigger alert</li> <li>– Coordinate resource and communication</li> </ul>	<ul style="list-style-type: none"> <li>– <b>IT Manager</b> (TBC, delegate: IT Team Leader Sachien Dalvi 0563054162)</li> <li>– <b>QHSE &amp; BC Manager</b> (Ali Al Kharusi, 050 4184191)</li> <li>– <b>ACC Manager</b></li> </ul>
IT DR Team	Implementing DR Plan and recovery	<ul style="list-style-type: none"> <li>– <b>IT Manager</b> (TBC, delegate: IT Team Leader Sachien Dalvi 0563054162)</li> <li>– <b>IT Information Security Specialist</b> (Augustine Uzoigwe 055 336 9087)</li> <li>– <b>IT Team Leader</b> (Sachien Dalvi 056 305 4162)</li> </ul>

## 6. REQUIRED RESOURCES

Each member of the IT DR team requires:

- Mobile phone / SMS
- IT DR contacts list
- Veeam

In addition, each member of the IT DR Implementation Team requires:

- Backup Site Access (access to Warehouse building, and Warehouse Data Centre) or
- Backup Site Remote Access via VPN and Internet
- Backup System Admin Account and Password
- IT DR Recovery procedures and critical applications startup priority lists

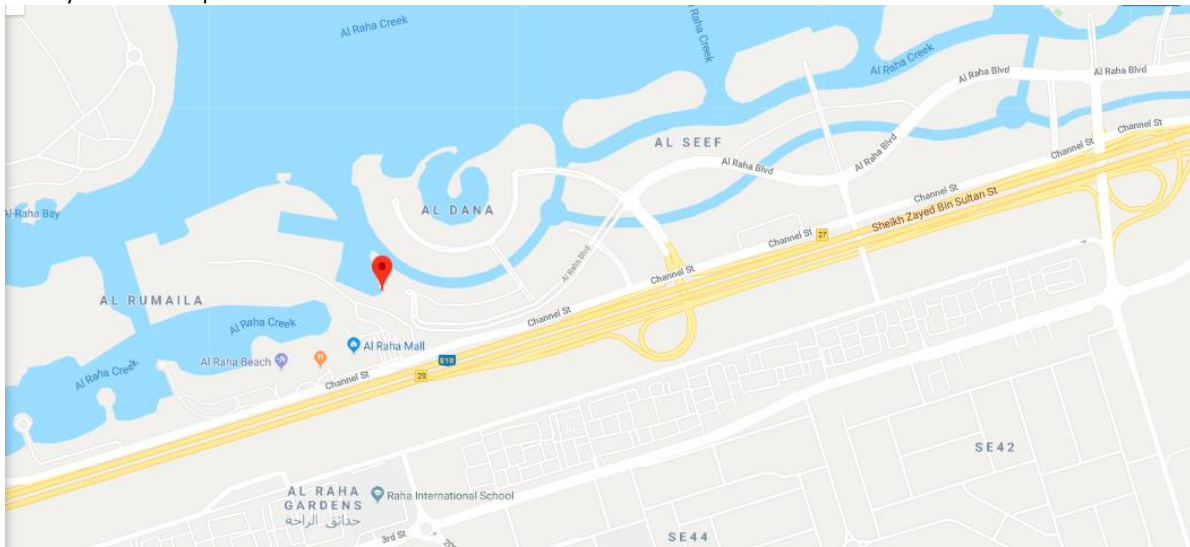
## 7. PRIMARY, SECONDARY, AND BACKUP LOCATIONS

### 7.1. PRIMARY LOCATION

National Ambulance Head Office  
13th Floor, Aldar HQ Building  
Al Raha Abu Dhabi

GPS Co-Ords: 24°26'28"N 54°34'31"E

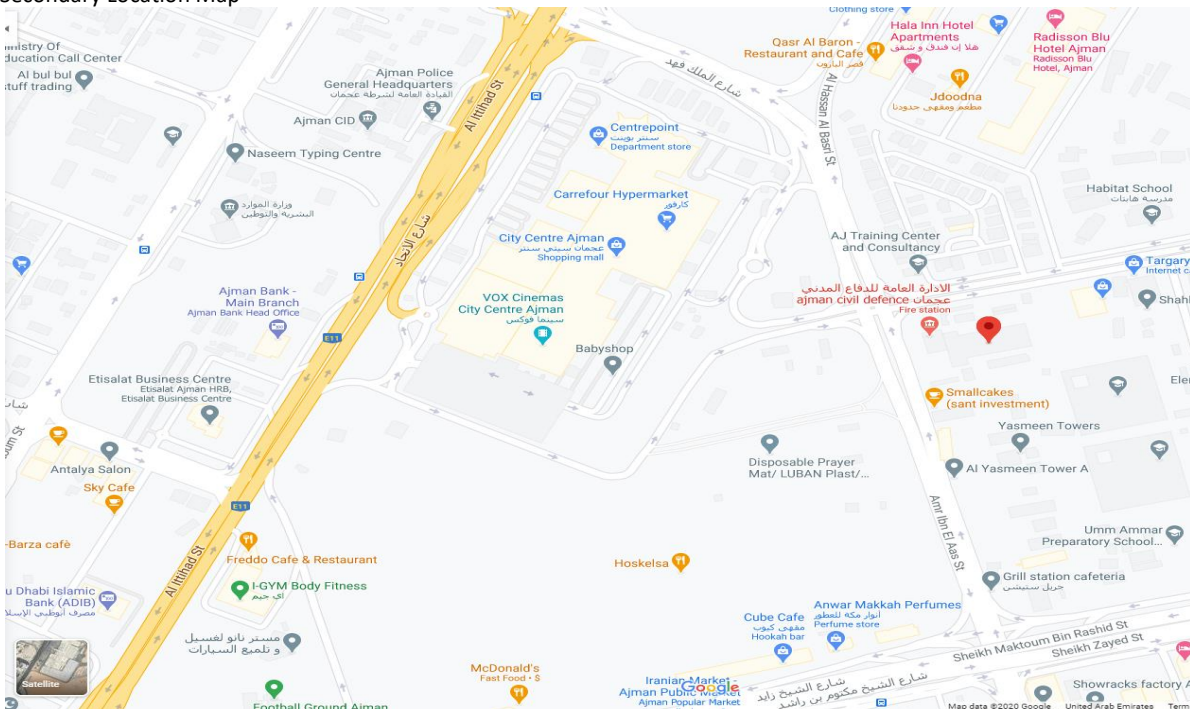
Primary Location Map



### 7.2. SECONDARY LOCATION

Ajman Civil Defence HQ  
GPS Co-Ords: 25.398387, 55.483438  
Plus Code 9FXM+98 Ajman

Secondary Location Map





### 7.3. BACKUP LOCATION

National Ambulance Warehouse KIZAD

GPS Co-Ords: 24.719520, 54.729726

Plus Code 7HPPPP9H+QQ

Backup Location Map



## 8. INTERESTED PARTIES

### 8.1. EXTERNAL INTERESTED PARTIES

Interested Party	Supplier/ Stakeholder	Services/ Products Provided	Name & Contact Details	Response Time (if applicable)
Etisalat	Supplier	PRI Lines MPLS Line Internet Lease Line	Helpdesk: 800 9111 Santosh Ramakrishnan (Account Manager): 050 233 3729	
AGC	Supplier	AVAYA IPT	Abdullah Savad: +971 52 120 2976 Helpdesk: 04 364 9009 <a href="mailto:customercare.mea@agcnetworks.com">customercare.mea@agcnetworks.com</a>	4 hr
Emircom	Supplier	Exsi Server VMWARE / Veeam / NetAPP Storage	Account Manager - Fouzi Raslan: +971 50 44 383 28 Helpdesk: nochelpdesk@emircom.com <a href="mailto:support.mea@dimensiondata.com">support.mea@dimensiondata.com</a> Phone (24 X 7) - Within UAE: +971 4 326 2539	4 hr
Softec / SafeCity	Supplier	CAD	Mayda: 055 157 1720 Tarek: 052 398 2229	4 hr
Smart360tech	Supplier	CISCO IPT	Heldesk – Paul: <a href="mailto:support@smart360tech.com">support@smart360tech.com</a> Phone 8x5: 04 294 3329 Mobile 24x7: 055 392 4081 Symantec Tech Support: 055 315 0615	4 hr
Symantec Antivirus Manager	Supplier	Antivirus Manager	Symantec Tech Support: 800 0441 2244	
KIT	Supplier	HO / DR / KIZAD Datacenter APC UPS and APC AC	Business Manager – IT Services, Saravanan Arumugam: +971 50 7780791	
HelpAG	Supplier	CISCO Iron Port	UAE: 800 HELPAG (435724) Dubai: 04 440 5666, Abu Dhabi: 02 644 <a href="mailto:support@helpag.com">support@helpag.com</a> <a href="http://www.helpag.com">http://www.helpag.com</a> Divjot Arora : 055 626 9780 Asim Sharfuddin - Manager Service Operations: 050 684 0181 <a href="mailto:asim.sharfuddin@helpag.com">asim.sharfuddin@helpag.com</a> Director Operations - Soeren Kroh : 055 414 4628 <a href="mailto:soeren.kroh@helpag.com">soeren.kroh@helpag.com</a> General Manager - Stephan Berner: 050 640 4574 <a href="mailto:stephan.berner@helpag.com">stephan.berner@helpag.com</a>	
Moi TETRA Radio Support	Service Provider	TETRA Radio Support	Moi TETRA Support AD 050 999 6878 ATLAS TETRA Support 052 698 9245 Col Hannie Moi Comms 050 999 1332	
VEEAM Support	SW Vendor	VEEAM software Support	800035703954 <a href="https://www.veeam.com/update.html">https://www.veeam.com/update.html</a>	



## 8.2. INTERNAL INTERESTED PARTIES

Name	Role in Plan	Office Number	Phone Number	Email
CEO (Ahmed Al Hajeri)	As determined in the roles and responsibilities table			AAIHajeri@nationalambulance.ae
CAMO (Dr Ayman Ahmad)				AAhmad@nationalambulance.ae
CFO (Charles Arnestad)				CArnestad@nationalambulance.ae
Operations Director (Dr Firas Al Kurdi)		02 596 8777	050 720 6633	FAIKurdi@nationalambulance.ae
IT Manager (TBC, Delegate: IT Team Leader)				
ACC Manager (Waseem Khan)		02 596 8611	050 736 1791	WKhan@nationalambulance.ae
QHSE & BC Manager (Ali Al Kharusi)		02 596 8624	050 4184191	AAIKharusi@nationalambulance.ae
IT Information Security Specialist (Augustine Uzoigwe)		02 596 8623	055 336 9087	AUzoigwe@nationalambulance.ae
IT Team Leader (Sachien Dalvi)		02 596 8690	056 305 4162	SDalvi@nationalambulance.ae

## 9. AUTHORITY TO ACTIVATE

- Any National Ambulance Executive acting individually may trigger the IT BC (DR) plan, or any procedures with the IT BC (DR) Plan.
- A National Ambulance Director plus the ACC Manager or IT Manager may trigger the IT DR (BC) plan, should an executive not be available at the time of the incident leading to the trigger.

## 10. CRITERIA FOR ACTIVATING

IT BC (DR) procedures should be triggered when one of the following criteria is met (or confidently anticipated), resulting in IT services being disabled or the provision of IT services from the primary location unstable or at a high risk of failure:

- Physical loss or lack of access to primary location: fire, flood, or other environmental conditions such as storms, building or access road closure.
- Extended loss of power, cooling: ADDC failure, district cooling failure, electrical failures
- Loss of ACC telephony or network at the primary location (Head Office).
- Software, hardware or other failure: service provider network outage phone or internet network provider failure (Etisalat), software licensing, hardware failure, or malicious activities such as hacking, computer virus or worm, denial of service attack or other cyber attack.

## 11. PLAN ACTIVATION AND IMMEDIATE RESPONSE PROCEDURE

Designations authorized to activate this plan may activate DR by calling one of the following staff members and instructing them to implement the IT DR Plan:

- IT Manager
- ACC Manager
- QHSE & BC Manager

The nature of the incident necessitating DR plan activation and any additional information as may be required to assist in execution should be provided.

The IT Manager or ACC Manager will then start mobilizing the IT DR team as required to activate the plan.

## 12. PRIORITIZED ACTIVITIES

The services will be prioritized in the following order:

Service	DR Method	IMPACT
1. <b>Telephony (998) services</b>	Multiple sites, Active-Active fully redundant	Zero public impact. Fully redundancy. NA Impacted for up to 3 Minutes at any one site
2. <b>Internet connectivity</b>	Multiple sites, Active-Active fully redundant	
3. <b>Critical Applications</b>	Multiple sites, Active-Standby 15 min recovery	Zero public impact. NA Impacted for up to 15 Minutes during recovery

The IT DR team will be tasked to test and verify the fully redundant services (telephony and internet) before starting to recover the critical applications.

## 13.IMPACT OF DISRUPTION ON PRIORITIZED ACTIVITIES OVER PREDETERMINED TIMEFRAME

Public access services will not be impacted during failover,

All critical services will automatically failover to or be recovered within 15 minutes of the DR plan being triggered, individual sites may revery to fallback systems while main systems are being recovered.

## 14.RESUMPTION OF PRIORITIZED ACTIVITIES

Operational Procedures for resuming prioritized activities depends on the failed service and is managed through their individual plans taking into account the timings of the IT service recovery / failover targets.

## 15. RETURN TO BUSINESS AS USUAL

Once the emergency / incident has ended or the event which triggered the implementation of DR has been resolved, the following steps will be taken by the IT Manager, QHSE Manager or ACC Manager, with assistance from the IT DR team, in order to return to normal operations:-

- 1- An assessment of the Primary Site as to its suitability to resume IT services
- 2- An assessment of hardware, software and data and it current state
- 3- Draft a recovery plan to address any issues found in the above assessments
- 4- Inform the IT DR Team of any issues which would prevent recovery
- 5- Agree and implement the recovery plan

On completion of the recovery plan, the IT DR Team will meet and review the following areas with a view to improving processes and removing issues and root causes from the environment.

- 1- Review the cause of the incident to determine if it could have been avoided and assess the likelihood of reoccurrence
- 2- Review the IT DR Plan, assess what worked and what can be improved
- 3- Review the incident log and activities to implement DR, assess what worked and what can be improved
- 4- Assess whether normal operations has been achieved and detail any outstanding issues to be resolved.

## 16. TESTING

Testing will be carried out according to the Test Schedule below. A Test Plan will be developed for each test, based on a review of past service outages, incident logs and incident register affecting IT services and service criticality. Staff members and third-parties responsible for planning, conducting and reviewing test outcomes will be identified. Advance notification of the plan will be issued to operations that may be affected by testing, and commencement of testing will be authorised by the IT Manager.

Testing types may range in complexity, risk and resources required:

- Desktop review – plan owner review existing arrangements and documents;
- Desktop walkthrough – IT DR team review plan step by step, may involve third-parties;
- Scenario testing – a test scenario is developed and workshoped with IT DR team;
- Partial or full simulation
- Live testing – eg full physical drill and shutdown of services.

### 16.1. IT SERVICE TEST SCHEDULE

Service/ Equipment	Test Type	Objective	Frequency / Quarter
Telephony (998) services	Partial simulation	Test Phone system and 998 redundancy	Quarterly
Internet connectivity	Partial Simulation	Test Internet redundancy	Q2
Critical Applications	Desktop Review	Ensure all procedures are up to date	Q2
	Partial simulation	Ensure DR processes are working	Q2
Data Backup	Partial simulation	Test Restore of Critical Data	Monthly

## 17. DOCUMENTATION AND RECORDS

National Ambulance approved documents (Forms/ Templates) are to be filled for maintaining records. Communications shall be done through email or other documented means whenever possible. IT forms and templates. Where possible a log of all DR activity will be maintained to review once the DR event is over.

## 18. RELEVANT LEGISLATION

International, federal or local legislation and circulars relevant to this Policy. Full detail on this legislation can be found in QHP109 Legal Register.

Code, Name of Legislation	Jurisdiction
NCMA 7000:2021 Standard	UAE

## 19. RELATED POLICIES AND FORMS

List related policies and procedures to the created/updated policy.

Policy & Procedure /Form

## 20.FEEDBACK

Any feedback or suggestions for improvement to this Policy, Processes or Procedures can be submitted to [qhse@nationalambulance.ae](mailto:qhse@nationalambulance.ae)

## 21.DOCUMENT CONTROL AND OWNERSHIP

A review and update of this document will take place as necessary, when changes occur that identify the need to revise this Policy such as changes in roles and responsibilities, release of new legislative or technical guidance, or identification of a new policy area.

This document ownership for editing is identified as:

- QHSE & BC Manager

### Change Brief

Version No.	Date	Change
1.0	April 2017	<i>New document</i>
2.0	July 2022	<i>Rewrite of the document</i>

---

CEO Approval

---

Board Member Verification

## APPENDIX A - Avaya IP Telephony (IPT) Phone System

### Introduction

Prior to carrying out a controlled failover of the AVAYA telephony system from the Aldar HQ servers to the Warehouse servers, to ensure no service outage a change request must be prepared and authorized. The change request must be:

- Planned with input from the ACC Manager and IT Manager
- Communicated to the ACC Team Leaders and Operations Director
- State the dates and times for the planned failover activity
- IT staff must be present at both sites prior for the duration of the activity, and
- Approved by top management

In the event of a problem with the failover exercise, major incident or high ACC call volumes, the ACC Manager or ACC Team Leader can stop the process, in order to prevent impact on the 998 service.

### Aim

The aim of this procedure is to set out the conditions and procedures required to:

- (a) Failover the Avaya IPT phone system from the NA Head Office to the Warehouse or Secondary site, and
- (b) Failback the Avaya IPT phone system from the Warehouse or Secondary site to the Head Office without loss of phone services.

### Overview

National Ambulance's AVAYA phone system is a fully redundant active – active system, with passive backup, IPT phone system with phone lines, gateways and call managers at Head Office (Aldar HQ building), Seconrary site (Ajman CD HQ) and Warehouse locations.

Under normal operating conditions for the IT and phone systems, the Head Office call managers are the primary systems in use. The Call Managers accept calls from both active gateways with the PRIs also being active-active.

Although the phone system is redundant, it can take up to 2-3 minutes for the secondary system to come online if the primary system is 'down' (ie it has failed) or is unresponsive.

In event that a total system failure occurs, there is a secondary CISCO IPT Phone system and second phone for key critical phone users (ACC). This process is outside the scope of this procedure.

It is important to realize that the National Ambulance network is required to work for the phones to operate properly. The phone system comprises of 5 main components running over the National Ambulance network (below).

### Phone System Components:

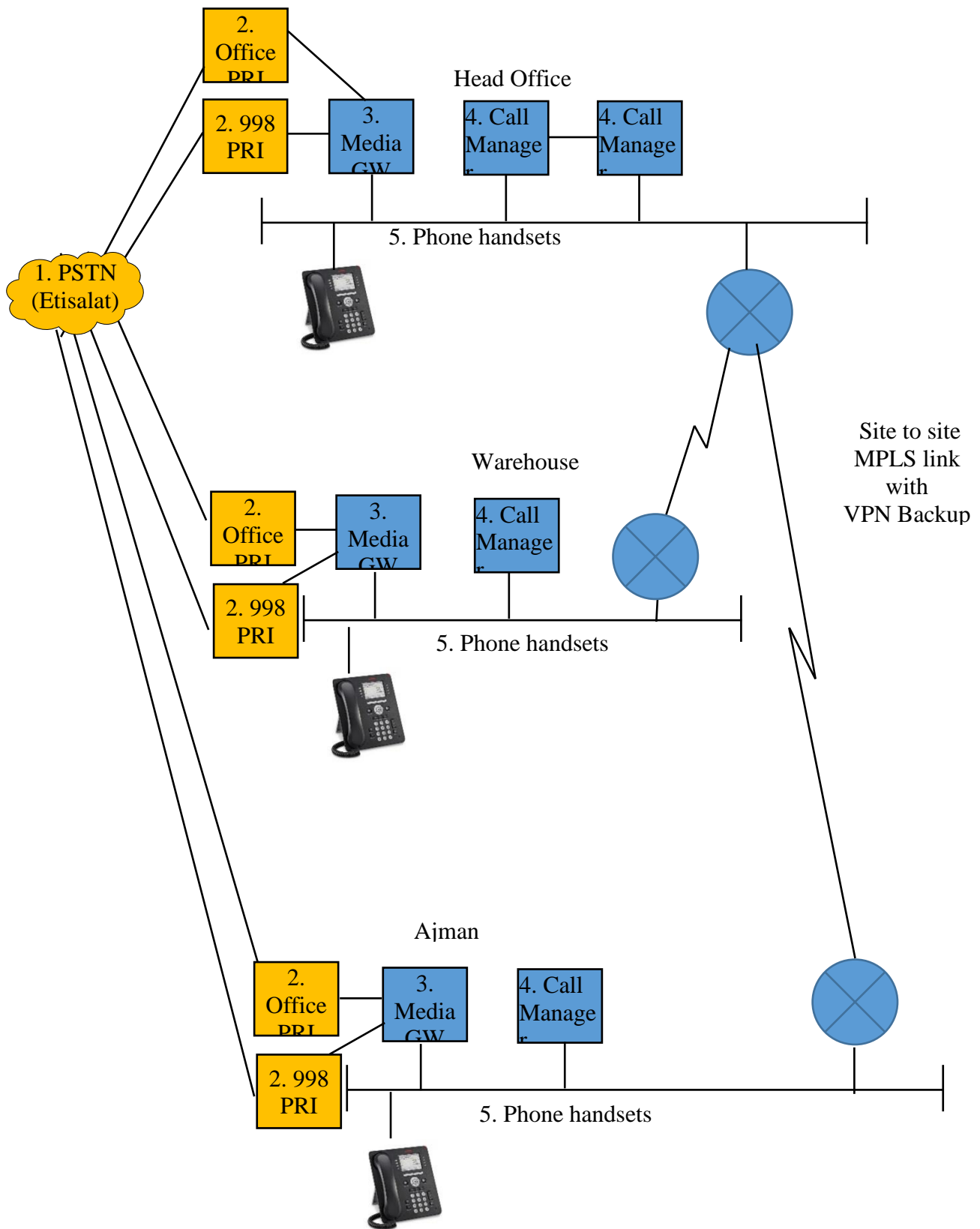
1. PSTN – The public phone network provided by Etisalat
2. PRI – The connection from the public phone network into NA office
3. Media Gateway ('Gateway') – The connection from the PRI to the NA Phone system
4. Call Manager – The AVAYA phone call management system (a server)
5. Phone Handsets

### Phone System Dependencies:

1. Power in the both Data Centers (phones are supported by the UPS in both locations)
2. IP Network (the IP of IPT)
3. Inter-site Link (MPLS)
4. Etisalat PSTN cloud connection to other networks



AVAYA Phone System Overview – Multiple Site Active-Active Redundancy:



## PROCEDURE – AVAYA PHONE FAILOVER

In order to ensure no outage of the 998 service, the following steps must be completed in the order specified below (Steps 1 – 24):

1. Ensure the network is operating between sites, and that both call manager systems are available (do a ping test)
2. Setup the Warehouse ACC computers to use the VPN / Sierra WIFI service to access CAD, and ensure the Head Office ACC backup systems (laptops, mobile phones and radios) are ready to use (refer to ACC procedures)
3. Call ACC Team Lead and verify that there are no 998 calls in progress. If there are 998 calls in progress – wait and ask ACC Team Leader to advise when all calls are complete and confirms it is okay to proceed with this activity.

Assuming that there are no 998 calls in progress, then:

4. Unplug the KIZAD incoming 998 PRI lines from the gateway to prevent 998 calls to the KIZAD (2 x lines)
5. Test 998 by calling 06998 from a mobile phone.

If 998 is working, proceed to the next step (Step 6), else if 998 is not working, reinstate the 998 PRIs lines by plugging them back in, retest (go to Step 5), and then stop or escalate the situation as appropriate.

6. Call ACC Team Leader to ensure that there are **no** 998 calls currently in progress. If there are 998 calls in progress – wait, and ask ACC Team Leader to advise when they are complete and confirm okay to proceed.
7. Unplug the site link (MPLS) at the Warehouse to isolate the Warehouse phone system
8. Wait for the KIZAD ACC phones to reconnect to the Warehouse call manager (this may take up to 4 minutes)
9. Verify the KIZAD phones are able to make calls by calling a mobile phone from KIZAD ACC phones.

Assuming the phones are working normally (ie able to make an outside call) then:

10. Reinstate the 998 PRIs by plugging them back in
11. Ask the KIZAD ACC staff to login to the 998 queue
12. Call ACC Team Leader and verify that there are no 998 calls in progress. If there are 998 calls in progress, wait until the ACC Team Leader advises all calls are finished and that this activity can proceed.

Assuming there are **no** 998 calls are in progress, then:

13. Unplug the Head Office incoming 998 PRIs line (2 x lines)
14. Unplug the network for Head Office call managers (2 x servers)
15. Test 998 by calling 06998 from a mobile phone.

If 998 is working then proceed to the next step, else reverse the steps taken by proceeding from Step 15 back to Step 1, retest 998, and then stop or escalate as appropriate.

16. Reinstate the site link (MPLS) to recombine the network
17. Test CAD access over the normal network at both the Warehouse ACC and Head Office ACC.

Assuming CAD is working proceed to Step 18, else reverse the steps taken by proceeding from Step 17 back to Step 1, retest, and then stop or escalate as appropriate.

18. Wait for the phones in the Head Office to reconnect to the Warehouse call manager (this may take up to 6 minutes)
19. Verify the Head Office ACC phones are able to make calls by calling a mobile phone
20. Test 998 by calling 06998 from a mobile phone.

Assuming 998 is working proceed to the next step (Step 21), else reverse the steps taken by proceeding from Step 20 back to Step 1, retest 998, and then stop or escalate as appropriate.

21. Ask the Head Office ACC staff to login to the 998 queue
22. Reinstate the Head Office incoming 998 PRI lines

23. Test 998 by calling 06998 from a mobile phone.

Assuming 998 is working proceed to the next step (Step 24), else reverse the steps taken by proceeding from Step 23 back to Step 1, retest 998, and and stop or escalate as appropriate.

24. Send out email communication to stakeholders (ACC, ACC Manager, Silver Command, IT Manager) confirming the ACC phones have failed over to the Warehouse.

**End of Procedure.**

## PROCEDURE – AVAYA PHONE FAILBACK

In order to ensure no outage of the 998 service, the following steps must be completed in the order specified below (Steps 1 – 26):

1. Ensure the network is operating normally between sites (do a ping test)
2. Setup the Warehouse ACC computers to use the VPN / Sierra WIFI service to access CAD, and ensure the Head Office ACC mobile backup equipment (laptops, mobile phones and radios) is ready to use (refer ACC procedures)
3. Call ACC Team Leader and verify that there are no 998 calls in progress. If there are 998 calls in progress, wait for the ACC Team Leader to advise when all calls are complete and that it is okay to proceed with this activity.

Assuming there are no calls are in progress, then:

4. Unplug the Head Office incoming 998 PRI lines (2 x lines) from the gateway to prevent 998 calls going to the Warehouse ACC
5. Test 998 by calling 06998 from a mobile phone.

Assuming 998 is working proceed to Step 6, else reinstate the 998 PRIs by plugging them back in, retest 998 and finish (end procedure), or escalate as appropriate.

6. Call ACC Team lead and verify that there are **no** 998 calls in progress. If there are 998 calls in progress, wait for the ACC Team Leader to advise when all calls are complete and that it is okay to proceed with this activity.

Assuming no calls are in progress then:

7. Unplug the site link (MPLS) at the Warehouse to isolate the Warehouse ACC phone system
8. Reinstate the Head Office call managers by plugging them back in
9. Wait for the phones in the Head Office to reconnect to the Head Office call manager (this may take up to 6 minutes)
10. Verify the Head Office ACC phones are able to make calls by calling a mobile phone
11. Test 998 by calling 06998 from a mobile phone.

Assuming 998 is working proceed to the next step, else reverse the steps taken by proceeding from Step 11 to Step 1, retest 998, and finish (end of procedure) or escalate as appropriate.

12. Ask the Head Office ACC staff to login to the 998 queue
13. Reinstate the Head Office 998 PRI lines
14. Test 998 by calling 06998 from a mobile phone.

Assuming 998 is working proceed to the next step (Step 15), else reverse the steps taken by proceeding from Step 14 back to Step 1, retest 998, and then stop (end of procedure), or escalate as appropriate.

15. Call ACC Team Leader and verify that there are no 998 calls in progress. If there are 998 calls in progress, wait for the ACC Team Lead to advise when all calls are complete and that it is okay to proceed with this activity.

Assuming there are no 998 calls in progress then:

16. Unplug the 2 x incoming Warehouse 998 PRI lines from the gateway to prevent 998 calls to the Warehouse
17. Test 998 by calling 06998 from a mobile phone.

Assuming 998 is working proceed to the next step (Step 18), else reinstate the 998 PRIs by plugging them back in, retest 998, and finish (end of procedure) or escalate as appropriate.

18. Reinstate the site link (MPLS) to recombine the network
19. Test CAD access over the normal network

Assuming CAD is working proceed to the next step (Step 20), else reverse the steps taken by proceeding from Step 19 – Step 1), retest 998 and finish (end of procedure) or escalate as appropriate.

20. Wait for the Warehouse ACC phones to reconnect to the Head Office call managers (this may take up to 6 minutes)
21. Verify the Warehouse ACC phones are able to make calls by calling a mobile phone from a phone in the Warehouse ACC
22. Test 998 by calling 06998 from a mobile phone.

Assuming 998 is working proceed to the next step (Step 23), else reverse the steps taken by proceeding from Step 22 – Step 1), retest 998 and finish (end of procedure) or escalate as appropriate.

23. Ask the Warehouse ACC staff to login to the 998 queue
24. Reinstate the 2 x Warehouse 998 PRI lines by plugging them back in
25. Test 998 by calling 06998 from a mobile phone.

Assuming 998 is working proceed to the next step, else reverse the steps taken by proceeding from Step 25 – Step 1), retest 998 and finish (end of procedure) or escalate as appropriate.

26. Send email communication to stakeholders (ACC, ACC Manager, Silver Command, IT Manager) confirming the ACC phones have failed over to the Head Office.

**End of Procedure.**



## APPENDIX B – Turning Data Centres Off/On

### PROCEDURE - SWITCHING 'OFF' THE ALDAR DATA CENTER

#### Background

A UPS provides backup power to the Aldar Data Centre. If there is a mains power failure, the UPS will continue to support Aldar Data Centre operations for up to 6 hours, however, this is dependent on the UPS battery status and it should not be assumed without checking during a power failure.

If mains power is not restored and there is 2 hours or less of battery life remaining on the UPS, prepare to migrate services to the Warehouse Data Centre in preparation for shutdown of the Aldar Data Centre (see procedure below).

#### Aldar Data Centre - Components & Equipment List

- Virtual Machine (VM) (there are several different types)
- Blade Server (UCS Host)
- UCS Chassis
- NetAPP Disk Shelf
- Storage Controller
- Fabric Interconnect

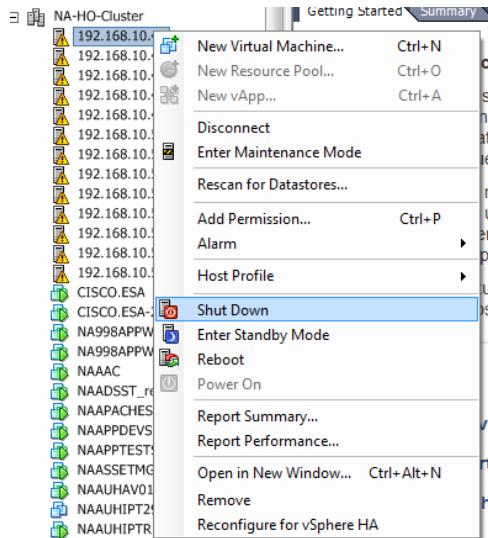
#### Preliminary Steps

For a planned shutdown of Aldar Data Centre, prepare a **Change Request** and obtain approval from CEO, DCEO, CAO, Operations Director, ACC Manager. The Change Request must address:

- Completion of a full data back up as close as possible to the scheduled shutdown start time (for unplanned Data Centre shutdown, additional data backup outside of the daily scheduled backup is not likely to be possible).
- Communication to all staff (Operations and Support) prior to start of the Shutdown, including alternatives for essential services where possible (email, phone).

#### Start of Procedure:

1. Prior to commencement of shutdown/ startup, inform the ACC Team Leader and check if any are 998 calls are in progress. If there are any calls in progress, wait for the ACC Team Leader to advise it is okay to proceed.
2. Shutdown all VMs in the following order:
  - (i) Web servers
  - (ii) App servers
  - (iii) DB servers
  - (iv) File servers
  - (v) Management servers
  - (vi) System (DHCP/ DNS /DC)
3. Using the vSphere web application, switch 'OFF' all UCS Hosts one by one, except the UCS Host which has a vCenter machine  
Vcenter VM IP – 192.168.10.43
4. Login to UCS Host (it hosts vCenter), and shutdown vCenter, and then that Host.



5. Shutdown the Proxy Server (x 1).



6. Remove the power cable from the UCS Chassis (there is no power switch, simply remove the cable)



7. Remove power cable from Fabric Interconnect (there is no power switch, simply remove the cable).



8. Switch off the Storage controller and Netapp Disk Shelf , it is on the same box and Remove power cable from Storage Controller of the NETAPP.





## PROCEDURE - SWITCHING 'ON' THE ALDAR DATA CENTRE

1. Plug in the power cable for the NetAPP Disk Shelf, and then the power cable for the Storage Controller. Turn 'ON' the power for each. Wait for 10 minutes before proceeding to the next step.



2. Plug in the power cable for the Fabric Interconnect. Wait for 10 minutes before proceeding to the next step.



3. Plug in the power cable to the UCS Chassis. Wait for 10 minutes.



4. Turn on the Proxy Server (x 1).



5. Login to UCS Host (it hosts the vCenter), and switch 'ON' the vCenter VM.



6. Using the vSphere Client application, login to vCenter Server.

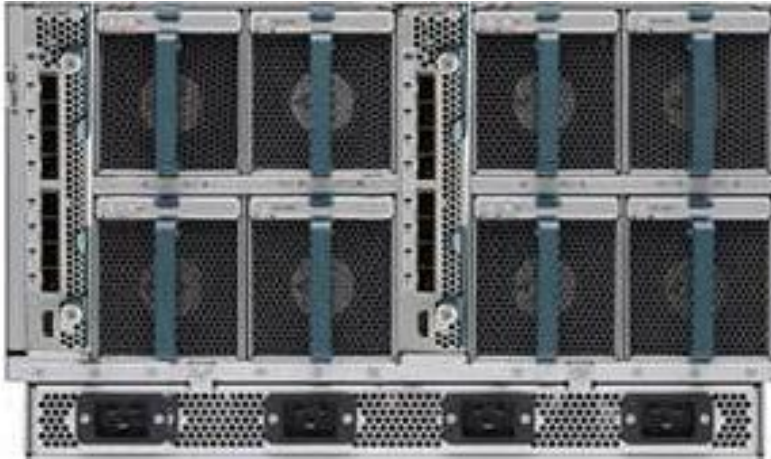
7. Turn on all VMs in the following order:

- (i) System (DC /DNS/DHCP)
- (ii) Management servers
- (iii) File servers
- (iv) DB servers
- (v) App servers
- (vi) Web servers



## PROCEDURE - SWITCHING 'OFF' THE WAREHOUSE DATA CENTER

1. Login to DR vCenter Server IP address 192.168.10.190 VM Name - NA-DR-VC01 through vSphere client:
  - Username - administrator@vsphere.local
  - Password – (IT team member will know – call IT Helpdesk if necessary).
2. Keep the vCenter VM and the Blade server related to this VM 'ON'. Shutdown the rest of the VMs one by one, and the remaining 3 x blade servers.
3. After shutting down all VMs and the 3 x blade servers, shutdown the vCenter VM.
4. Login to the fourth blade server and switch off this blade server too.
  - Username - root
  - Password – (IT team member will know – call IT Helpdesk if necessary).
5. Remove the 4 x power cables from the UCS Chassis (there is no power switch, simply remove the cable). See image below.



6. Remove the 4 x power cables from Fabric Interconnect (there is no power switch, simply remove the cable) (see image below).



7. Switch off the Storage Controller, and then switch off the Netapp Disk Shelf , it is on the same box (see image below).



8. Remove the 2 x power cables from Storage Controller of the NETAPP (see image above).
9. If necessary, then switch off all the below Physical Servers.
  - (i) NADRBKUP server (use screen menu or press power button).
  - (ii) NADR Proxy server (use screen menu or press power button).
  - (iii) NADRDC01 server (use screen menu or press power button).

## PROCEDURE - SWITCHING 'ON' THE WAREHOUSE DATA CENTRE

1. Turn 'ON' the Active Directory (AD) server and DHCP server (both are on the same machine). The host name for this server is NADRDC01 server.
2. Turn 'ON' the NetAPP Storage Controller and Disk Shelf (2 x power switches) (see image below). Wait for 10 minutes.



3. Put the 4 x power cables back into the Fabric Interconnect (see image below). Wait for 5 minutes.



4. Put the 4 x power cables back into the UCS BLADE Server (see image below). Wait for 10 minutes.



5. Login in to the Blade Server that has a vCenter VM, and then switch 'ON' the vCenter VM. The vCenter Server IP address 192.168.10.190

- Username - administrator@vsphere.local
- Password – (IT team member will know – call IT Helpdesk if necessary).

6. If the Backup and Proxy Servers are 'OFF', turn both of them back 'ON'.

**End of Procedure.**

## APPENDIX C – Data Recovery

### Overview

National Ambulance is using the **Veeam** backup and replication tool to recover the VM. This tool offers number of recovery option for various disaster recovery scenarios.

- VM Recovery enables you to instantly start a VM directly from a backup file.
- Guest OS and Data file Recovery enables you to recover individual guest OS files from Windows, Linux, Mac and other guest OS file systems.

### Components / Equipment:

- VEEAM backup machine at Warehouse DR Data Centre
- VEEAM proxy machine at Aldar HQ Data Centre
- VEEAM proxy machine at Warehouse DR Data Centre



## PROCEDURE - VM RECOVERY

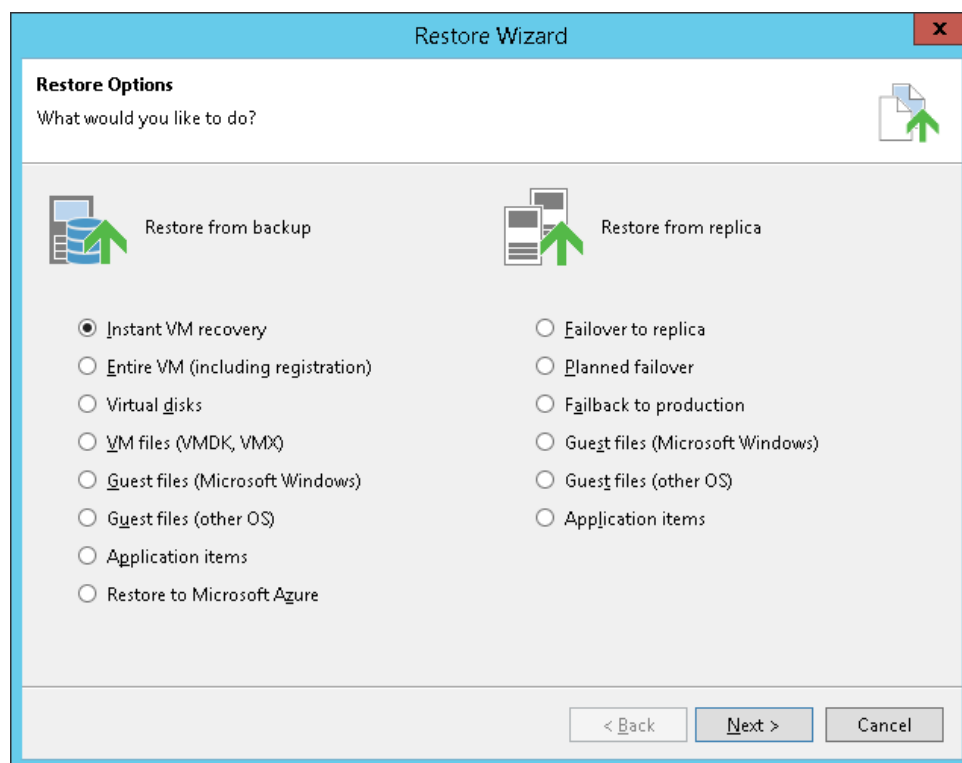
Enables you to instantly start a VM directly from a backup file. Immediately start a VM from a backup file stored on the backup repository.

### Start of Procedure:

#### Step 1. Launch Instant VM Recovery Wizard

To launch the **Instant VM Recovery** wizard, do one of the following:

- On the **Home** tab, click **Restore** and select **VMware vSphere backup**. In the **Restore from backup** section, select **Instant VM recovery**.
- Open the **Home** view, in the inventory pane select **Backups**. In the working area, expand the necessary backup, select the VM you want to restore and click **Instant VM Recovery** on the ribbon.
- Open the **Home** view, in the inventory pane select **Backups**. In the working area, expand the necessary backup, right-click the VM you want to restore and select **Instant VM recovery**.





## Step 2. Select VMs

At the **Virtual Machine** step of the wizard, select the VM that you want to recover:

1. In the **VM to recover** list, expand the backup job.
2. Select the VM.

To quickly find a VM, you can use the search field at the bottom of the window.

1. Enter a VM name or a part of it in the search field.
2. Click the **Start search** button on the right or press **[ENTER]**.

Instant Recovery

**Virtual Machine**  
Choose the virtual machine you want to recover.

Virtual Machine	VM to recover: NAC-DC.NAC.ae_replica_replica																																																																				
Restore Point	<table border="1"> <thead> <tr> <th>Job name</th> <th>Last restore point</th> <th>VM count</th> <th>Restore points count</th> </tr> </thead> <tbody> <tr> <td>Backup Job 11</td> <td>5/19/2018 9:30:49 PM</td> <td>13</td> <td></td> </tr> <tr> <td>Backup Job DHCP</td> <td>3/7/2018 9:45:17 PM</td> <td>2</td> <td></td> </tr> <tr> <td>Backup Job Mailbox ...</td> <td>5/31/2018 4:30:24 PM</td> <td>2</td> <td></td> </tr> <tr> <td>Backup_APP1_VM_HQ</td> <td>5/25/2018 5:00:27 PM</td> <td>3</td> <td></td> </tr> <tr> <td>Backup_APP2_VM_HQ</td> <td>5/25/2018 5:15:28 PM</td> <td>6</td> <td></td> </tr> <tr> <td>  NAC-DC.NAC.ae_...</td> <td>less than a day ago (7...</td> <td></td> <td>9</td> </tr> <tr> <td>  NADHCP01</td> <td>less than a day ago (7...</td> <td></td> <td>9</td> </tr> <tr> <td>  NAHUBCAS02</td> <td>less than a day ago (7...</td> <td></td> <td>9</td> </tr> <tr> <td>  NACADC</td> <td>less than a day ago (7...</td> <td></td> <td>9</td> </tr> <tr> <td>  NADHCP02</td> <td>less than a day ago (7...</td> <td></td> <td>9</td> </tr> <tr> <td>  NAHUBCAS01</td> <td>less than a day ago (7...</td> <td></td> <td>9</td> </tr> <tr> <td>Backup_APP3_VM_HQ</td> <td>5/25/2018 5:40:34 PM</td> <td>7</td> <td></td> </tr> <tr> <td>Backup_APP4_VM_HQ</td> <td>5/25/2018 6:00:40 PM</td> <td>8</td> <td></td> </tr> <tr> <td>Backup_APP5_VM_HQ</td> <td>5/25/2018 6:15:18 PM</td> <td>6</td> <td></td> </tr> <tr> <td>Backup_APP6_VM_HQ</td> <td>5/25/2018 7:00:55 PM</td> <td>6</td> <td></td> </tr> <tr> <td>Backup_APP7_VM_HQ</td> <td>5/11/2018 7:10:00 PM</td> <td>6</td> <td></td> </tr> </tbody> </table>	Job name	Last restore point	VM count	Restore points count	Backup Job 11	5/19/2018 9:30:49 PM	13		Backup Job DHCP	3/7/2018 9:45:17 PM	2		Backup Job Mailbox ...	5/31/2018 4:30:24 PM	2		Backup_APP1_VM_HQ	5/25/2018 5:00:27 PM	3		Backup_APP2_VM_HQ	5/25/2018 5:15:28 PM	6		NAC-DC.NAC.ae_...	less than a day ago (7...		9	NADHCP01	less than a day ago (7...		9	NAHUBCAS02	less than a day ago (7...		9	NACADC	less than a day ago (7...		9	NADHCP02	less than a day ago (7...		9	NAHUBCAS01	less than a day ago (7...		9	Backup_APP3_VM_HQ	5/25/2018 5:40:34 PM	7		Backup_APP4_VM_HQ	5/25/2018 6:00:40 PM	8		Backup_APP5_VM_HQ	5/25/2018 6:15:18 PM	6		Backup_APP6_VM_HQ	5/25/2018 7:00:55 PM	6		Backup_APP7_VM_HQ	5/11/2018 7:10:00 PM	6	
Job name	Last restore point	VM count	Restore points count																																																																		
Backup Job 11	5/19/2018 9:30:49 PM	13																																																																			
Backup Job DHCP	3/7/2018 9:45:17 PM	2																																																																			
Backup Job Mailbox ...	5/31/2018 4:30:24 PM	2																																																																			
Backup_APP1_VM_HQ	5/25/2018 5:00:27 PM	3																																																																			
Backup_APP2_VM_HQ	5/25/2018 5:15:28 PM	6																																																																			
NAC-DC.NAC.ae_...	less than a day ago (7...		9																																																																		
NADHCP01	less than a day ago (7...		9																																																																		
NAHUBCAS02	less than a day ago (7...		9																																																																		
NACADC	less than a day ago (7...		9																																																																		
NADHCP02	less than a day ago (7...		9																																																																		
NAHUBCAS01	less than a day ago (7...		9																																																																		
Backup_APP3_VM_HQ	5/25/2018 5:40:34 PM	7																																																																			
Backup_APP4_VM_HQ	5/25/2018 6:00:40 PM	8																																																																			
Backup_APP5_VM_HQ	5/25/2018 6:15:18 PM	6																																																																			
Backup_APP6_VM_HQ	5/25/2018 7:00:55 PM	6																																																																			
Backup_APP7_VM_HQ	5/11/2018 7:10:00 PM	6																																																																			
Recovery Mode																																																																					
Restore Reason																																																																					
Ready to Apply																																																																					
Recovery																																																																					

Type in an object name to search for

< Previous Next > Finish Cancel

## Step 3. Select Restore Point

At the **Restore Point** step of the wizard, select the restore point for the VM.

Instant Recovery
×

**Restore Point**  
Choose restore point you want to recover the selected virtual machine to.

Virtual Machine
Restore Point
Recovery Mode
Restore Reason
Ready to Apply
Recovery

VM name: **NAC-DC.NAC.ae\_replica\_replica**      Original host: **navcentre01.nac.ae**  
VM size: **112.3 GB**  
Available restore points:

Created	Type
less than a day ago (7:54 PM Monday 6/4/2018)	Increment
2 days ago (7:54 PM Saturday 6/2/2018)	Increment
3 days ago (7:56 PM Friday 6/1/2018)	Full
4 days ago (7:47 PM Thursday 5/31/2018)	Increment
5 days ago (7:51 PM Wednesday 5/30/2018)	Increment
6 days ago (7:45 PM Tuesday 5/29/2018)	Increment
7 days ago (8:09 PM Monday 5/28/2018)	Increment
9 days ago (7:35 PM Saturday 5/26/2018)	Increment
10 days ago (7:41 PM Friday 5/25/2018)	Full

< Previous
Next >
Finish
Cancel

#### Step 4. Select Recovery Mode

At the **Recovery Mode** of the wizard, choose the necessary restore mode:

- Select **Restore to the original location** if you want to restore the VM with its initial settings and to its original location. If this option is selected, you will pass directly to the Restore step of the wizard.
- Select **Restore to a new location, or with different settings** if you want to restore the VM to a different location and/or with different settings (such as VM location, network settings, format of restored virtual disks and so on). If this option is selected, the **Instant Recovery** wizard will include additional steps for customizing VM settings.

#### IMPORTANT!

If you recover a VM with original settings, and the original VM still exists in the virtual infrastructure, the original VM will be removed.

Virtual Machines

Restore Mode

Reason

Summary

Restore Mode

Specify whether selected VMs should be restored back to the original location, or to a new location or with different settings.

☒ **Restore to the original location**  
 Quickly initiate restore of selected VMs to the original location, and with the original name and settings. This option minimizes the chance of user input error.

☐ **Restore to a new location, or with different settings**  
 Customize restored VM location, and change its settings. The wizard will automatically populate all controls with the original VM settings as the default settings.  
  
[Pick proxy to use](#)

☒ Restore VM tags  
 Select this option to restore VM tags that were assigned to the VM when backup was taken.

☒ Quick rollback (restore changed blocks only)  
 Allows for quick VM recovery in case of guest OS software problem, or user error. Do not use this option when recovering from disaster caused by hardware or storage issue, or power loss.

< Previous

Next >

Finish

Cancel

#### Step 5. Verify Instant VM Recovery Settings

At the **Ready to Apply** step of the wizard, specify additional settings for Instant VM Recovery:

1. If you are recovering a production VM that has failed and want to restore it with initial network settings, select the **Connect VM to network** check box. If you are recovering a VM for testing disaster recovery while the initial VM is still running, leave this check box not selected. Before you power on such VM, you will have to manually change VM network settings: disconnect the VM from the production network and connect it to an isolated non-production network to avoid conflicts.
2. To start a VM immediately after recovery, select the **Power on VM automatically** check box. If you are recovering the VM to the production network, make sure that the initial VM is powered off to avoid conflicts.
3. Check settings you have specified for Instant VM Recovery and click **Next**. Veeam Backup & Replication will recover the VM on the selected ESX(i) host.

**CERTIFIED**  
**LR**  
ISO 9001 • ISO 14001  
ISO 45001



## PROCEDURE - GUEST OS FILE OR DATA FILE RECOVERY

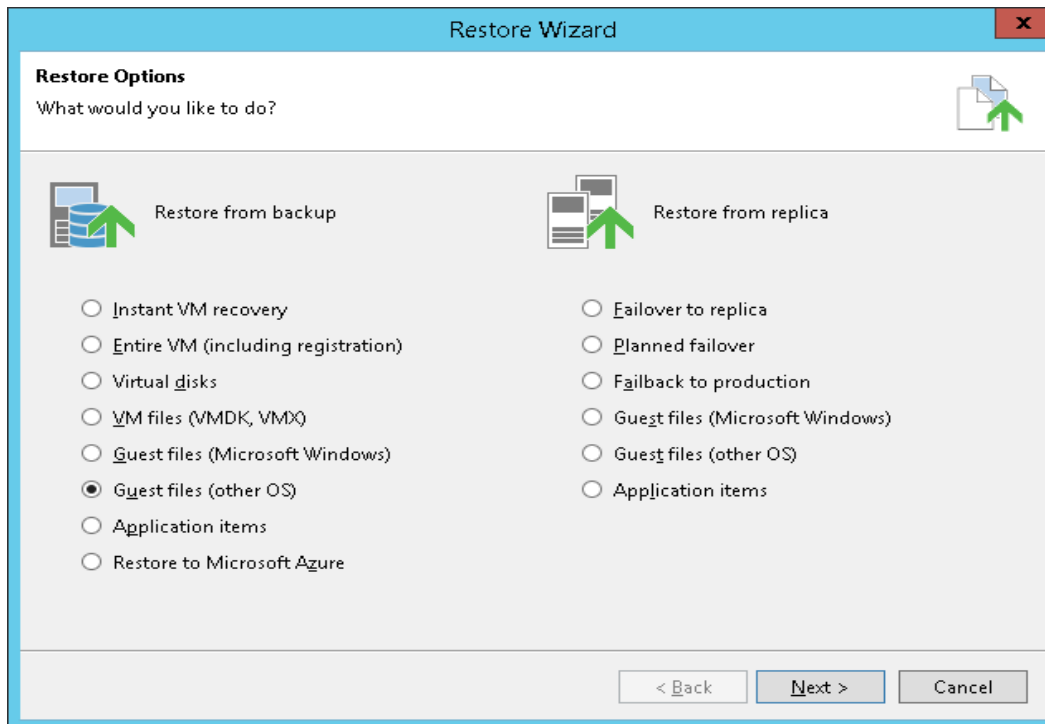
This enable to recover of files and folders only

### Step 1. Launch Veeam File Level Restore Wizard

To launch the **Guest File Restore** wizard, do one of the following:

- On the **Home** tab, click **Restore** and select **VMware vSphere backup**. In the **Restore from backup** section, select **Guest files (other OS)**.
- Open the **Home** view, in the inventory pane select **Backups**. In the working area, expand the necessary backup, select the VM whose guest OS files you want to restore and click **Guest Files > Linux and other** on the ribbon.
- Open the **Home** view, in the inventory pane select **Backups**. In the working area, expand the necessary backup, right-click the VM whose guest OS files you want to restore and select **Restore guest files > Linux and other**.
- Double-click the VBK or VBM file (for example, in Microsoft Windows Explorer). In the displayed window, select the VM and click **Restore > Guest files (Linux and other)**.

You can use this option if you perform restore on the backup server. You cannot use this option if you perform restore via the Veeam Backup & Replication console.



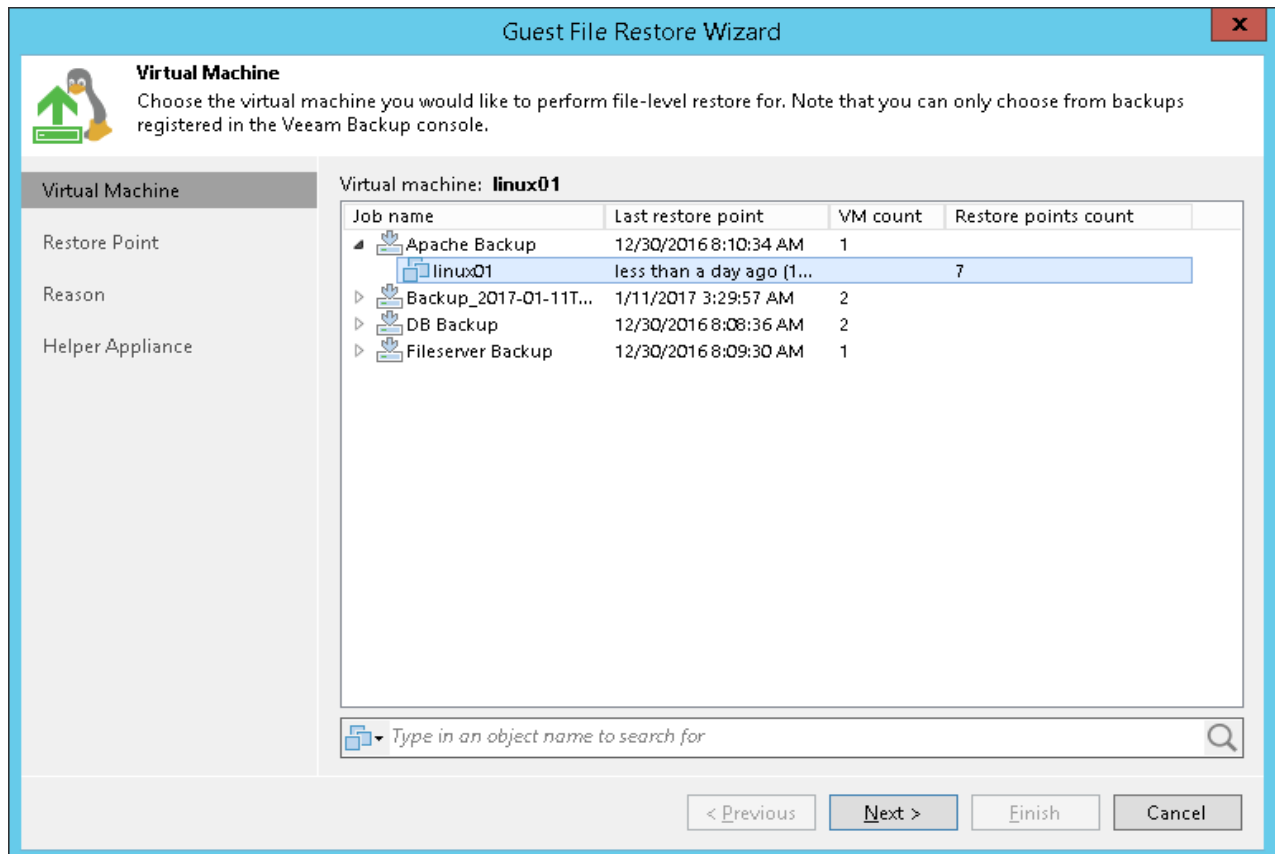
## Step 2. Select VM

At the **Virtual Machine** step of the wizard, select the VM whose guest OS files you want to restore:

1. In the **Virtual machine** list, expand the necessary backup.
2. Select the VM.

To quickly find a VM, you can use the search field at the bottom of the window.

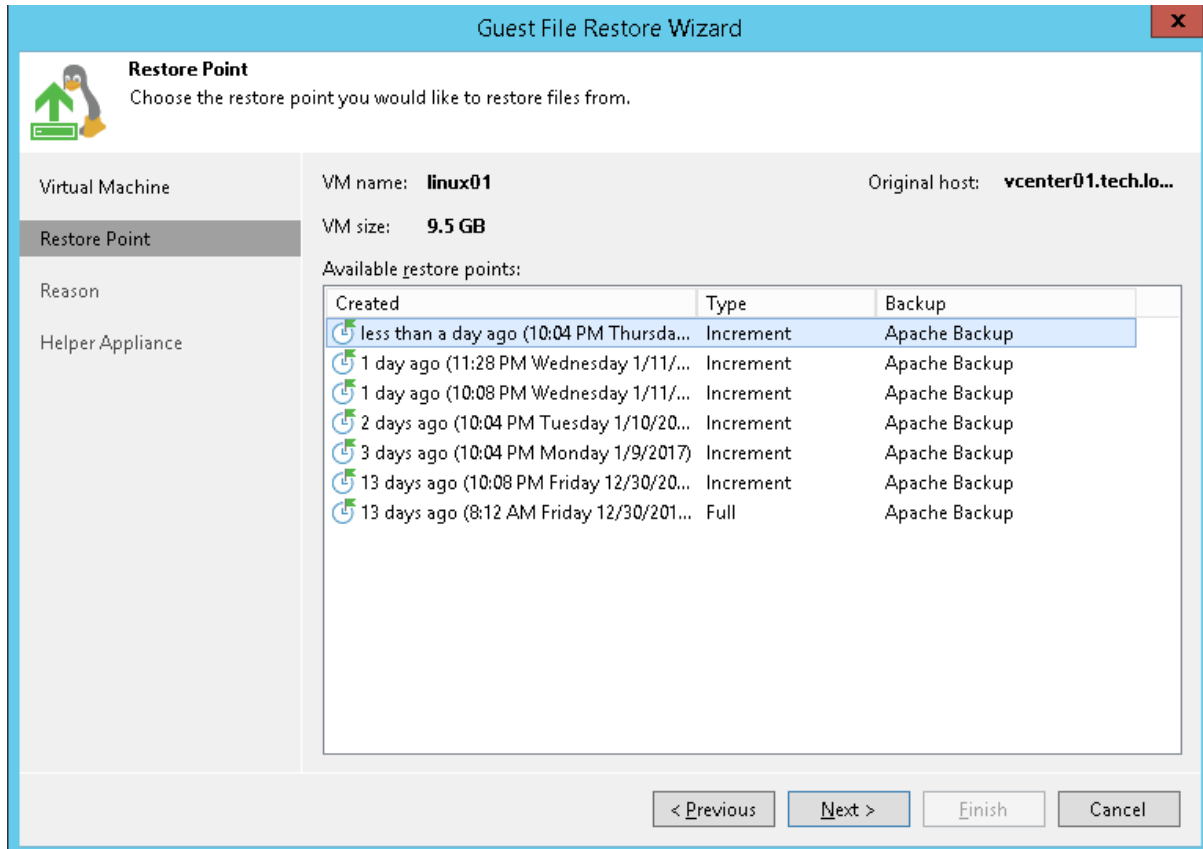
3. Enter a VM name or a part of it in the search field.
4. Click the **Start search** button on the right or press [ENTER].



## Step 3. Select Restore Point



At the **Restore Point** step of the wizard, select the restore point from which you want to restore VM guest OS files



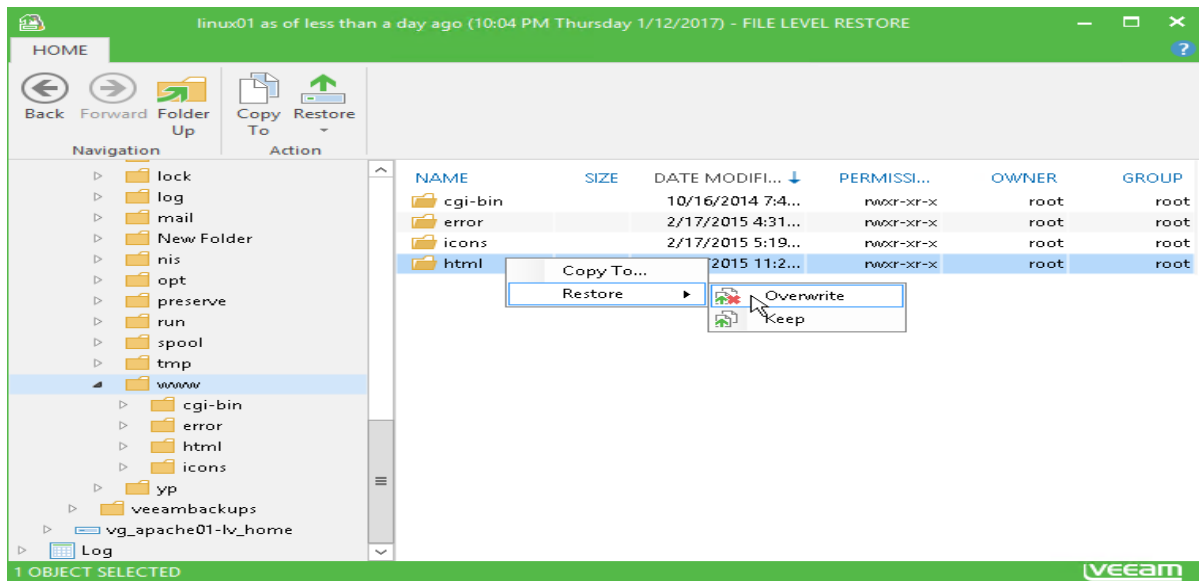
#### Step 4. Save Restored Files

##### Restoring Files to Original Location

To restore files and folders to the original location, right-click the necessary file or folder in the file system tree or in the details pane on the right and select one of the following commands:

- To overwrite the original file on the VM guest OS with the file restored from the backup, select **Restore > Overwrite**.
- To save the file restored from the backup next to the original file, select **Restore > Keep**. Veeam Backup & Replication will add the **RESTORED-** prefix to the original file name and store the restored file in the same folder where the original file resides.

To restore files to the original location, Veeam Backup & Replication uses the account for VM guest OS access specified in the backup job settings. If this account does not have sufficient rights to access the target VM, you will be prompted to enter credentials. In the **Credentials window**, specify a user account to access the destination location (server or shared folder).



In some cases, you may remove the original VM and restore it from the backup by the time of file-level restore. If you then attempt to restore VM guest OS files to the original location, **Veeam Backup & Replication** will not be able to find the original VM by its reference ID, and display a warning. Click OK and browse to the target VM in the virtual infrastructure to which you want to restore VM guest OS files.

[End of Procedure.](#)

## PROCEDURE - PLANNED FAILOVER

A planned failover is smooth manual switching from a primary VM to its replica with minimum interrupting in operation. You can use the planned failover, for example, if you plan to perform datacenter migration, maintenance or software upgrade of the primary VMs. You can also perform planned failover if you have an advance notice of a disaster approaching that will require taking the primary servers offline.

When you start the planned failover, **Veeam Backup & Replication** performs the following steps:

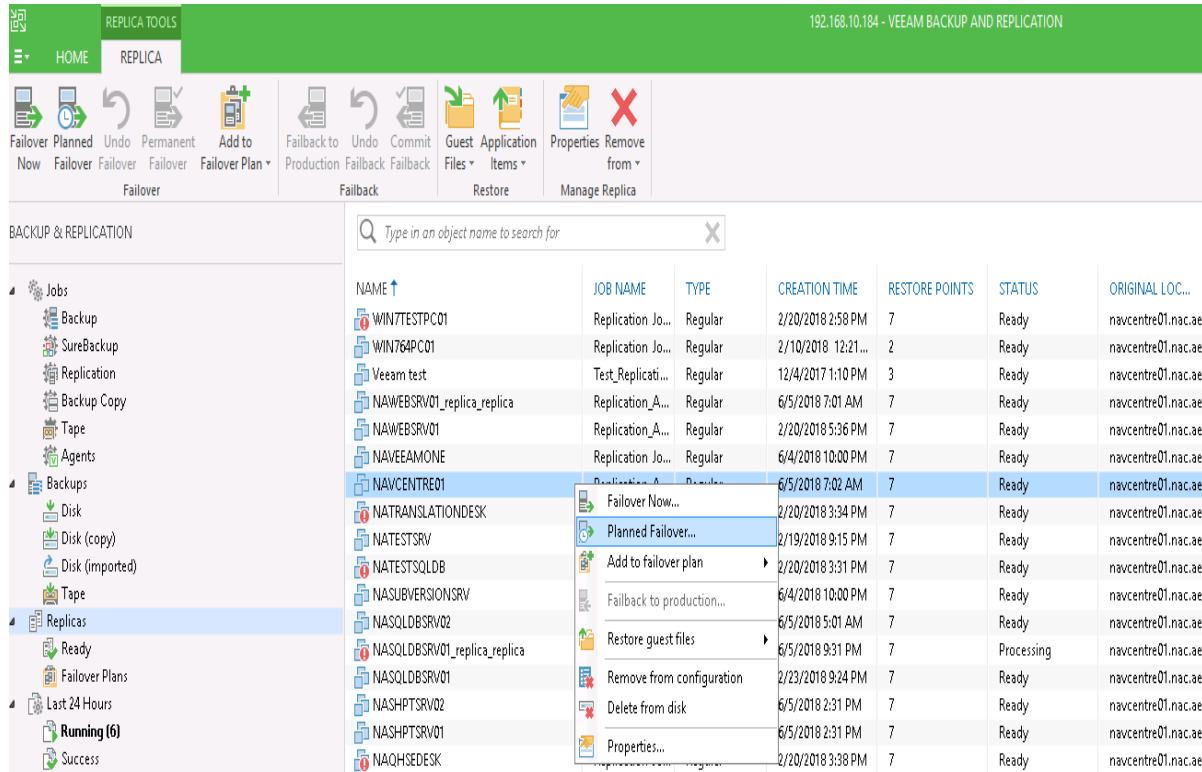
1. The failover process triggers the replication job to perform an incremental replication run and copy the un-replicated changes to the replica.
2. The VM is powered off.
3. The failover process triggers the replication job to perform another incremental replication run and copy the portion of last-minute changes to the replica. The replica becomes fully synchronized with the source VM.
4. The VM is failed over to its replica.
5. The VM replica is powered on

### Step 1. Launch Planned Failover Wizard

To launch the **Planned Failover** wizard, do one of the following:

- On the **Home** tab, click **Restore** and select **VMware**. In the **Restore from replica** section, select **Planned failover**.
- Open the **Home** view, expand the **Replicas** node. In the working area, select one or more VMs and click **Planned Failover** on the ribbon. You can also right-click one or more VMs and select **Planned Failover**.
- Open the **Inventory** view, in the working right-click one or more VMs area and select **Restore > Planned Failover**.

In this case, the selected VMs will be automatically included into the planned failover task. You can add other VMs to the task when passing through the wizard steps.



## Step 2. Select VMs

At the **Virtual Machines** step of the wizard, select one or more VMs for which you want to perform failover. You can perform failover for separate VMs and whole VM containers.

To select VMs and VM containers:

1. Click **Add VM**.
2. Select where to browse for VMs and VM containers:
  - **From infrastructure** — browse the virtual environment and select VMs or VM containers. If you choose a VM container, Veeam Backup & Replication will expand it to a plain VM list.

To quickly find VMs or VM containers, you can use the search field at the bottom of the **Add Object** window. Enter a VM or VM container name or a part of it in the search field and click **Start search** or press **[ENTER]**.

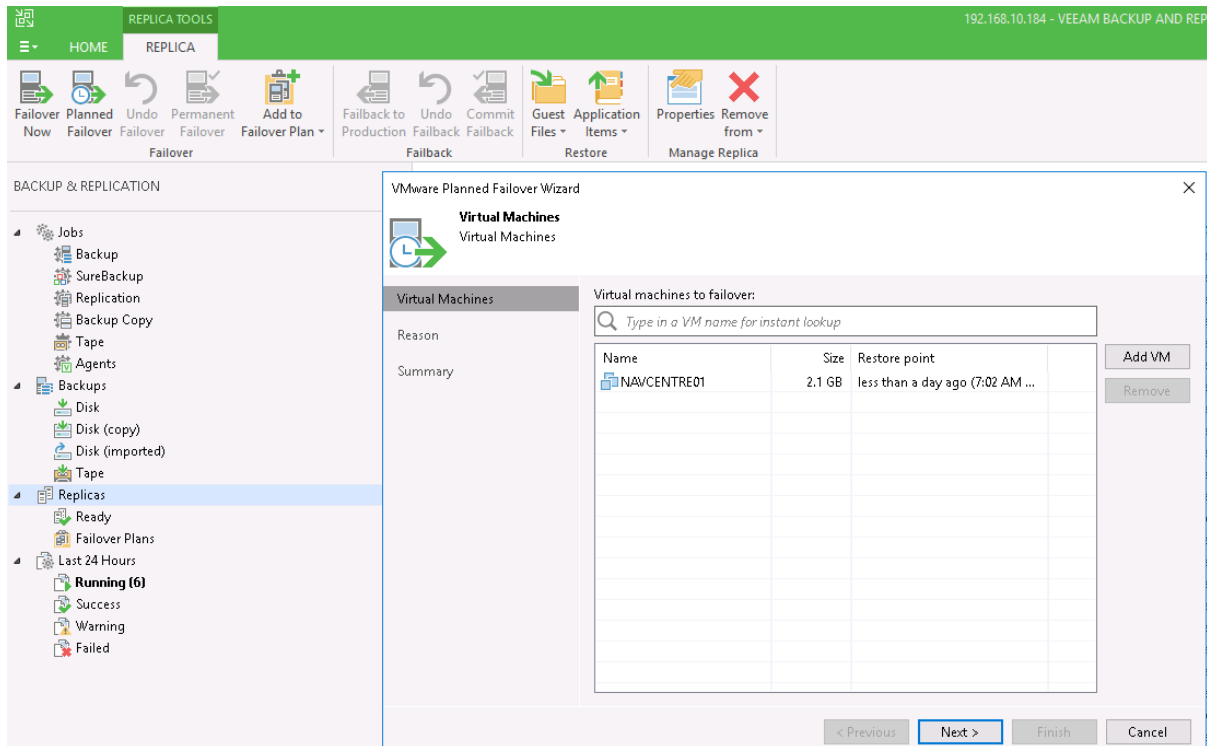
- **From replicas** — browse existing replication jobs and select all VMs or specific VMs from replication jobs.

To quickly find VMs, you can use the search field at the bottom of the **Backup Browser** window. Enter a VM name or a part of it in the search field and click **Start search** or press **[ENTER]**.

You can also use the search field at the top of the wizard:

1. Enter a VM name or a part of it in the search field. Veeam Backup & Replication will display possible matches.
2. If the VM is not in the list, click the **Show more** link to browse existing VM replicas. Veeam Backup & Replication will open the **Backup Browser** window, and you can select the necessary VM replica there.

Make sure that VMs you select from the virtual environment have been successfully replicated at least once.



### Step 3. Specify Failover Reason

At the **Reason** step of the wizard, enter a reason for failing over to the VM replica(s). The information you provide will be saved in the session history and you can reference it later.

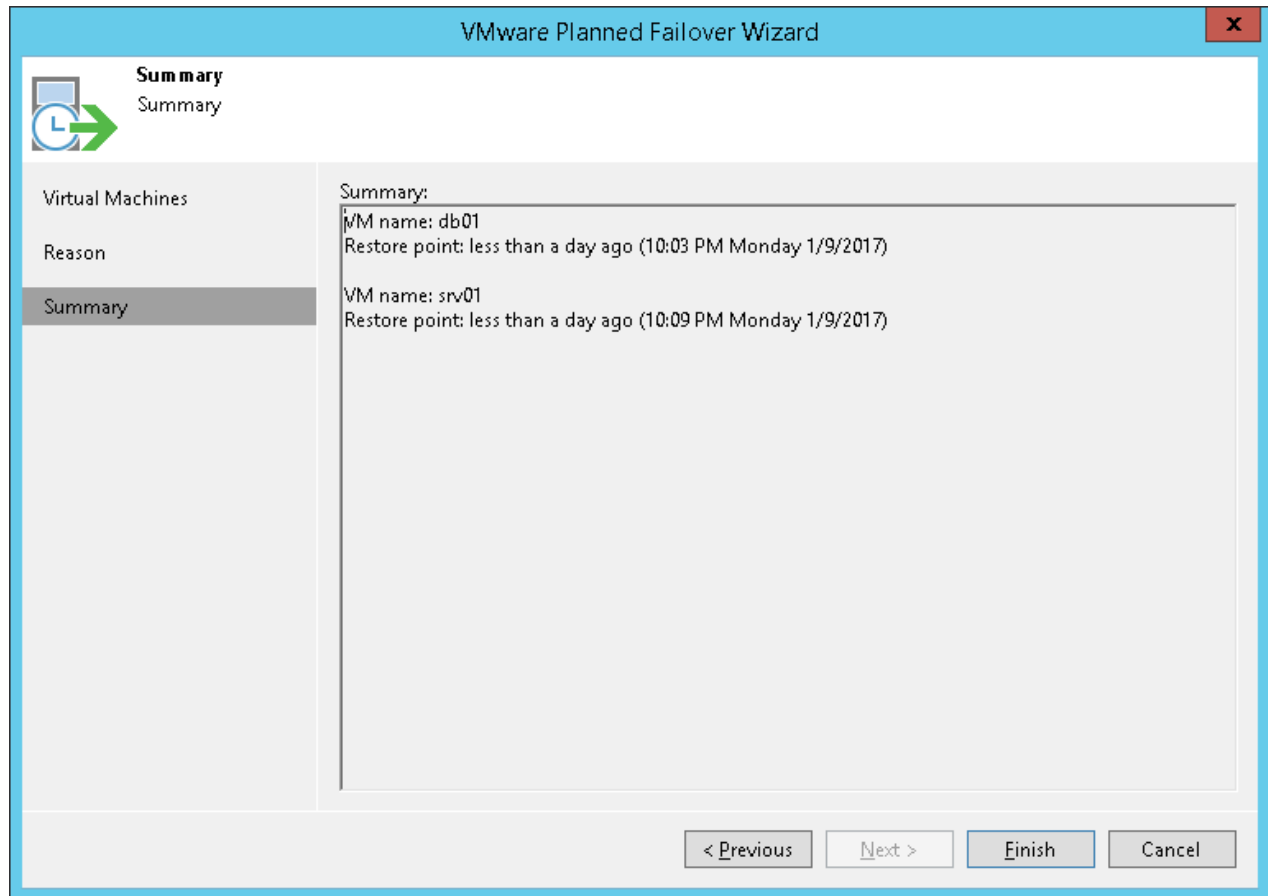


#### Step 4. Review Summary and Finish Working with Wizard

At the **Summary** step of the wizard, complete the procedure of planned failover.

1. Review details of the failover task.
2. Click **Finish** to start the failover process.

Once planned failover is complete, the VM replica(s) will be started on the target host(s).



End of Procedure.

## APPENDIX D – Network failover- public services

The Network is designed to be fully redundant in that local network services will failover to the backup site whenever the head office network is no longer available for whatever reason.

Public incoming services currently require an update to the Firewall policy to be allowed into the DR site, the procedure for enabling this is detailed below.

### PROCEDURE – ACTIVATING THE PUBLIC SERVICES IN NETWORK FAILOVER

When the Internet Leased Line in the Head Office fails or is switched off. The National Ambulance Public IP services like VPN, Kronos Access, LMS, Email, Starcomm tracking, 998 Apps, Google Maps Service ePCR Uploads, Internet access / Browsing etc. are automatically failed over to backup internet Leased Line at KIZAD Warehouse. But a manual Static Route Priority and Policy Based Route (PBR) need to be activated to make the traffic routed through the DR Internet.

IPv4 Virtual IP 30		
NA_EXCH_97_esa	94.56.139.97 --> 192.168.10.69 (TCP: 443 --> 443)	OutSide-Network (port6)
NA_eCLAIM_98	94.56.139.98 --> 192.168.10.34	OutSide-Network (port6)
NA_NA998_APP_99	94.56.139.99 --> 192.168.10.120	OutSide-Network (port6)
NA_ePCR_101	94.56.139.101 --> 192.168.10.22	OutSide-Network (port6)
NA_BIOMETRIC_102	94.56.139.102 --> 192.168.10.31	OutSide-Network (port6)
NATOTARA_103	94.56.139.103 --> 192.168.10.36	OutSide-Network (port6)
NA_GPS_104	94.56.139.104 --> 192.168.10.101	OutSide-Network (port6)
NA_ACC_105	94.56.139.105 --> 192.168.10.115	OutSide-Network (port6)
NA_GPS_106	94.56.139.106 --> 192.168.10.104	OutSide-Network (port6)
Avaya_Ports_110	94.56.139.110 --> 192.168.10.82	OutSide-Network (port6)
Avaya_Ports_111	94.56.139.111 --> 192.168.10.81	OutSide-Network (port6)
IT Asset	94.56.139.109 --> 192.168.10.30	OutSide-Network (port6)
Google Maps_107	94.56.139.107 --> 192.168.10.116	OutSide-Network (port6)
FTP_108	94.56.139.108 --> 192.168.10.137	OutSide-Network (port6)
IT Helpdesk	151.253.104.32 --> 192.168.10.27	OutSide-Network (port6)
ESA_NAT_SMTP	94.56.139.97 --> 192.168.10.25 (TCP: 25 --> 25)	OutSide-Network (port6)
ESA_NAT_POP3	94.56.139.97 --> 192.168.10.25 (TCP: 110 --> 110)	OutSide-Network (port6)
ESA_NAT_IMAP	94.56.139.97 --> 192.168.10.25 (TCP: 143 --> 143)	OutSide-Network (port6)
ESA_NAT_IMAPS	94.56.139.97 --> 192.168.10.25 (TCP: 993 --> 993)	any
Kronos_VIP	151.253.104.33 --> 192.168.10.139	OutSide-Network (port6)
LMS	151.253.104.34 --> 192.168.10.90	OutSide-Network (port6)
NA-ADMDM.NAC	151.253.104.35 --> 192.168.10.17	OutSide-Network (port6)
ADSelfservice	151.253.104.36 --> 192.168.10.245	OutSide-Network (port6)
Symantec_Public	151.253.104.37 --> 192.168.10.15	OutSide-Network (port6)
AD_Self Service	151.253.104.38 --> 192.168.10.32	OutSide-Network (port6)
Kronos_Clock_EXT	151.253.104.39 --> 192.168.10.134	OutSide-Network (port6)
AVAYA-CM	151.253.104.40 --> 192.168.90.26	OutSide-Network (port6)
MOI_Server	151.253.104.41 --> 192.168.10.129	OutSide-Network (port6)
NASERVICEDESK.nationalambulance.ae	151.253.104.42 --> 192.168.10.35	OutSide-Network (port6)
ADSS.nationalambulance.ae	151.253.104.43 --> 192.168.10.245	OutSide-Network (port6)

#### Publicly available services and their corresponding IP addresses Mapping

The below steps are followed to enable the Services to work.

- Login into the KIZAD WAREHOUSE firewall @https://10.200.16.14:8443
- Click on Network TAB and select Static Routes
- Select the Priority 1 Route as shown below, Click on Edit, change the 0 to 10
- Also select the Priority 2 Route and leave it as is "5" this makes the Backup line higher priority interface.

Note: Lower number of priority is better, hence 0 is better than 10 and would be take higher priority.

Destination	Gateway	Comment	Interface
0.0.0.0/0	151.253.136.49		OUTSIDE-INTERNET (port7)
0.0.0.0/0	151.253.159.76		OutSide-Network-BKP_IL (port8)

Static Route settings showing 151.253.136.49 as a Priority

Edit Static Route

Dynamic Gateway ☒

Destination

Subnet
Named Address
Internet Service

Interface

Gateway Address ☒

Gateway IP 151.253.136.49 could be unreachable. It is not in any subnet of the interface port7:

- 10.25.5.169/24

Administrative Distance

Comments  0/255

Status ☒ Enabled ☐ Disabled



Advanced Options

Priority

OK Cancel


Screen showing where to change the priority of the Route – This should be changed to 10

**Edit Static Route**


Dynamic Gateway  

Destination **Subnet** **Named Address** **Internet Service**



0.0.0.0/0.0.0.0

Interface  OutSide-Network-BKP\_ILL (port8)


Gateway Address 151.253.159.76

Administrative Distance  10

Comments Write a comment... 0/255

Status  Enabled  Disabled





**Advanced Options**

Priority  5

**OK** **Cancel**

Screen showing where to change the priority of the Route – This should be left as is to promote it to higher priority.

**FortiGate 501E** NAWH-FIREWALL01

Seq.#	Incoming Interface	Outgoing Interface	Source	Destination
1	Inside_Network	port8	192.168.10.69/255.255.255.255	0.0.0.0/0.0.0.0
2	Inside_Network	port8	192.168.10.34/255.255.255.255	0.0.0.0/0.0.0.0
3	Inside_Network	port8	192.168.10.122/255.255.255.255	0.0.0.0/0.0.0.0
4	Inside_Network	port8	192.168.10.22/255.255.255.255	0.0.0.0/0.0.0.0
5	Inside_Network	port8	192.168.10.31/255.255.255.255	0.0.0.0/0.0.0.0
6	Inside_Network	port8	192.168.10.36/255.255.255.255	0.0.0.0/0.0.0.0
7	Inside_Network	port8	192.168.10.101/255.255.255.255	0.0.0.0/0.0.0.0
8	Inside_Network	port8	192.168.10.115/255.255.255.255	0.0.0.0/0.0.0.0
9	Inside_Network	port8	192.168.10.104/255.255.255.255	0.0.0.0/0.0.0.0
10	Inside_Network	port8	192.168.10.82/255.255.255.255	0.0.0.0/0.0.0.0

Screen showing all the Inbound traffic routed back to internet using Policy based Routing, any newly added service need to be added here to enable it work during failover.

To add a new IP to the Policy Based Routes

1. Click on Network TAB and select Policy Routes
2. Select Add New, Select Protocol "ANY"
3. Select Incoming interface "Inside Network"
4. Enter the Private IP of the public Service e.g. email is 192.168.10.69
5. Select destination as all network "0.0.0.0/0"
6. Select action as "Forward Traffic"
7. Also select Outgoing Interface as "BKP-ILL"
8. Enter the Gateway Address as "151.253.159.76"
9. Click Okay to save



Edit Routing Policy

If incoming traffic matches:

Protocol
TCP
UDP
SCTP
**ANY**
Specify
0

Incoming Interface
Inside\_Network
+

Source Address
IP/Netmask
192.168.10.69/255.255.255.255
Addresses
+

Destination Address
IP/Netmask
0.0.0.0/0.0.0.0
Addresses
+

Type of Service
Bit Pattern
0x00
Bit Mask
0x00

Then:

Action
**Forward Traffic**
Stop Policy Routing

Outgoing Interface
OutSide-Network-BKP\_ILL (port#

Gateway Address
151.253.159.76

Comments
Email Outbound Return Traffic
29/255

Status
Enabled
Disabled

OK
Cancel

Screen showing where to add the Reverse route that send the return traffic through the right interface. Repeat the same for any additional service

After this change the WH will start receiving and forwarding traffics for externally hosted service.

[End Of Procedure](#)