



GIG  
CYMRU  
NHS  
WALES

Gwasanaeth  
Gwybodeg  
Informatics  
Service

Angerddol am wneud gwahaniaeth  
Darparu gwybodaeth a thechnoleg ar gyfer gofal gwell  
Passionate about making a difference  
Delivering information and technology for better care

159-20180803 – Active Directory System Failure Technical Report

# 159-20180803 - Active Directory System Failure Technical Report

*This report provides the technical findings into the Active Directory  
System Failure which occurred on 3<sup>rd</sup> August 2018*

Version No. 2.0  
Status: Approved

Author: Keith Reeves  
Approver: Carwyn Lloyd-Jones

Date: 17/08/2018

Tŷ Glan-yr-Afon  
21 Heol Ddwyreiniol Y Bont-Faen, Caerdydd CF11 9AD  
21 Cowbridge Road East, Cardiff CF11 9AD  
Ffôn/Tel: 02920 500500  
[www.cymru.nhs.uk/gwybodeg](http://www.cymru.nhs.uk/gwybodeg)  
[www.wales.nhs.uk/informatics](http://www.wales.nhs.uk/informatics)

-FINAL-

IF PRINTED THIS BECOMES AN UNCONTROLLED COPY

159-20180803 - Active Directory Major System Failure Technical Report v2.docx

Page 1 of 8

Author: Keith Reeves  
Approver: Carwyn Lloyd-Jones

## 159 – 20180803 Active Directory System Failure Technical Report

### TABLE OF CONTENTS

1	Introduction.....	3
2	Background and Terminology .....	3
3	Situation .....	4
4	Outcomes.....	6
4.1	Corrective Actions.....	6
4.2	Preventative Actions .....	6
	Appendix A Document History.....	7

**-FINAL-**

IF PRINTED THIS BECOMES AN UNCONTROLLED COPY

159-20180803 - Active Directory Major System Failure Technical Report v2.docx

Page 2 of 8

Author: Keith Reeves

Approver: Carwyn Lloyd-Jones

## 159 – 20180803 Active Directory System Failure Technical Report

### 1 Introduction

This interim report is in relation to the Active Directory System Failure which was experienced on 3<sup>rd</sup> August 2018.

This report reflects an initial technical assessment of the incident, based on information available at the time, and the steps taken to resolve it.

A further comprehensive review is underway to look at the incident that occurred, as well as any contributory factors, which may relate to the outage or any impact caused by it. This will include any previous occurrences or potential related events.

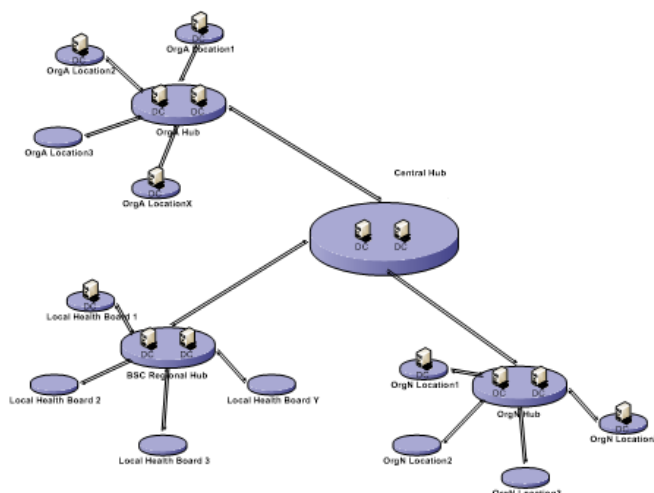
The outcome of the review will then be used to implement any changes necessary in order to prevent another similar failure, and to identify any lessons learned to lessen the impact of any future incidents.

### 2 Background and Terminology

#### Active Directory

The NHS Wales Active Directory deployment was originally configured based on a design developed for NHS Wales by Microsoft in 2007 and approved for implementation. This was reviewed and redesigned in 2014, in collaboration between Trustmarque and NHS Wales.

The approach taken satisfied the design principles laid out for the NHS Wales infrastructure at the time of deployment. A simplified diagram of the structure is as follows:



-FINAL-

## 159 – 20180803 Active Directory System Failure Technical Report

A central hub contains two domain controllers. This central hub is connected to organisational hubs, which contain further domain controllers, which connect to individual locations, which may contain further domain controllers. This forms what is known as a snowflake structure.

Any manipulation of data within the directory, which is made to the domain controllers in the central hub, is then replicated through the organisational hubs, and on to any further domain controllers located in connected locations.

This design offers the following benefits:

- Most flexible – allows for any restructuring
- Simplest – users cannot get confused which is their logon domain
- Easily allows for complete autonomy of each local organisation in respect to their resources – servers, workstations, user accounts, groups...
- Consistent – where it matters – while allowing local IT to enforce their decisions
- Allows to perform any low-level, technical AD administration (replication configuration and maintenance, etc.) only once – potential for cost saving
- Nation-wide, ideal platform for national messaging solution
- Can easily cope with the scale – 100,000+ users
- Last but not least, the design follows current Microsoft recommendations

### Domain Controllers

A domain controller is a server on a Microsoft Windows network that is responsible for the authentication, authorisation and enforcement of client policies. Each domain controller contains user account information to authenticate users, provide access, and enforce any security policies for a Windows domain.

### System Volume (SysVol)

The System Volume (SysVol) is a shared directory that sits on a domain controller and stores the server copy of the domain's policies and configuration that must be shared for common access and replication throughout a domain.

This folder also contains user login scripts and group policy objects, which set settings and parameters for users and computers (e.g. set proxy servers, disable access to certain settings, etc.).

## 3 Situation

-FINAL-

## 159 – 20180803 Active Directory System Failure Technical Report

At 21:42 on 2<sup>nd</sup> August 2018, a user in Cardiff and Vale identified an issue, where the email mailbox was missing from Active Directory for a single user. On further investigation, a wider issue in the National Active Directory was identified, where data was missing from within the database.

NWIS continued the investigation through the night in collaboration with their suppliers, and to resolve this issue the intention was to undertake a restore of the missing data from a backup, which had previously been taken prior to 11:00 on 2<sup>nd</sup> August 2018.

In order to restore the deleted objects, a restore of both the Active Directory database and SysVol took place. This was undertaken in conjunction with, and under guidance provided by, the supplier. Whilst the authentication element of Active Directory was seemingly unaffected, the 'SysVol' share attempted to perform a simultaneous replication of the restored data with all domain controllers, whilst the attempted restoration was taking place. This replication meant that SysVol was not consistent across all domain controllers within the domain as the restored files were replicated from the authoritatively restored copy.

This caused user disruption and loss of access to some National Services that primarily use thin client technology or Citrix as a method for users to access. In addition, there were local issues across Health Boards affecting some users, including loss of print capability, accessing local systems, and shared files and folders. The impact was variable in that some Local Health Boards and Trusts (LHBs) were affected more than others.

A Major Incident was declared at 08:49 on the 3<sup>rd</sup> August 2018, impacted support teams were convened, and LHBs and Welsh Government were made aware, whilst investigations and response plans were prepared.

A number of technical workarounds were implemented as interim measures by NWIS and the LHBs, to ensure that impact was minimised to end users. A number of technical and managerial conference calls were held throughout the event, with LHBs being communicated to at appropriate times.

At 15:00 on the 3<sup>rd</sup> August 2018, it was agreed between ADIs and NWIS to stop replication to prevent the issue spreading further.

A second managed restore and replication activity was then planned, in consultation with the NWIS supplier, and the ADIs, using the previous night's backup. This was agreed with ADIs and was scheduled to be undertaken, by NWIS and their supplier, over the weekend of the 4<sup>th</sup> and 5<sup>th</sup> of August 2018.

The restore and replication activity commenced at 12:30 on the 4<sup>th</sup> August and was completed on the 5<sup>th</sup> August at 20:05, restoring access to services albeit with some remedial activities required by Application Services following prior failover of Services.

-FINAL-

## 159 – 20180803 Active Directory System Failure Technical Report

The following National services had calls raised with the National Service Desk, which provided evidence of the impact of this outage.

- Canisc
- GP Test Requesting
- Hosted Messaging Service (email)
- INPS Vision
- Integration Services
- Welsh Clinical Portal including Welsh Care Records Service
- Welsh Laboratory Information Management Service

## 4 Outcomes

### 4.1 Corrective Actions

A number of technical workarounds were implemented as interim measures by NWIS and the LHBs, to ensure that access to business and clinical systems was restored as soon as possible.

Replication was stopped to prevent the issue spreading further.

A restore and replication activity was then undertaken on the SysVol contents to restore service.

### 4.2 Preventative Actions

NWIS, in consultation with the Infrastructure Management Board, approved a temporary Change freeze for Infrastructure Services for a period of seven days, to allow for monitoring and stable running.

-FINAL-

## 159 – 20180803 Active Directory System Failure Technical Report

### Appendix A Document History

#### A.1 Revision History

Date	Version	Author	Revision Summary
10/08/2018	0.1	Keith Reeves	First Draft
15/08/2018	0.2	Keith Reeves	Second Draft following peer review
15/08/2018	0.3	Keith Reeves	Clarification on points following peer review, and removal of track changes
16/08/2018	0.4	Keith Reeves	Amendments following response from Lead Infrastructure Design Architect
17/08/2018	V1.0	Keith Reeves	Submission to Directors for sign off
17/08/2018	V2.0	Keith Reeves	Amendments following review by Director of NHS Wales Informatics Service, Director of ICT, and Director of Application Development and Support.


#### A.2 Reviewers

This document requires the following reviews:

Date	Version	Name	Position
15/08/2018	0.2   0.3   0.4	Michelle Sell	Chief Operating Officer
15/08/2018	0.2   0.3   0.4	Simon Williams	Head of Service Management
15/08/2018	0.2   0.3   0.4	Steven Howlett	Principal Service Management Specialist
15/08/2018	0.2   0.3   0.4	David Rees	Service Management Specialist
15/08/2018	0.2   0.3   0.4	David Owen	Lead Infrastructure Design Architect
15/08/2018	0.2   0.3   0.4	Peggy Edwards	Head of Clinical & Informatics Assurance

#### A.3 Authorisation

Signing of this document indicates acceptance of its contents.

Author's Name:	Keith Reeves
Role:	Service Management Lead
Signature:	<div style="text-align: right;">17/08/2018</div> <div style="text-align: center;">  </div> <hr/> <div>             Keith Reeves              Service Management Lead              Signed by: Keith Reeves (Ke125547) </div>

-FINAL-

## 159 – 20180803 Active Directory System Failure Technical Report

Approver's Name:	Andrew Griffiths
Role:	Director of NHS Wales Informatics Service
Signature:	<p>17/08/2018</p> <p>X Carwyn Lloyd-Jones</p> <p>Carwyn Lloyd-Jones Director of ICT Signed by: Carwyn Lloyd-Jones (Ca000262)</p>

### A.4 Document Location

Type	Location
Electronic	

### A.5 Report Distribution (NWIS)

Title	Date	Audience
159-20180803 – Active Directory System Failure Technical Report v2	15/08/2018	<p>Director NHS Wales Informatics Service</p> <p>Director of ICT</p> <p>Director of Applications Development &amp; Support</p> <p>Chief Operating Officer</p> <p>Head of Clinical &amp; Informatics Assurance</p>

-FINAL-