NWC OT Cybersecurity Patch Management Detailed Design

National Water Company (NWC), KSA

SCADA/OT Information Security Implementation Project

Document Number:	A01001045-DLD-PM
Document Title:	NWC OT Cybersecurity Patch Management Detailed Design
Document Version:	1
NWC Contract No.:	101200487
[atm] PO Ref.:	ATMPO2020-034

1400 Broadfield Blvd Suite 200 Houston TX, 77084
Tel: +1 832 386 5593 | Fax: +1 832 201 0337
Email: sales@acetsolutions.com |
URL: www.acetsolutions.com

NOTES AND COPYRIGHTS

NWC has contracted this project to [atm] under contract number 101200487. ACET Solutions is the technical consultant of [atm] responsible for planning and execution of this project. All references to ACET Solutions in this document should be construed as [atm]/ACET Solutions for contractual purpose. Acceptance of this deliverable by NWC shall meet the requirements of the respective deliverable under NWC contract number 101200487.

Questions or comment regarding this deliverable should be directed to the ACET Solutions Project Director.

ACET Solutions LLC
1400 Broadfield Blvd Suite 200
Houston TX, 77084
Email: sales@acetsolutions.com | URL: www.acetsolutions.com

APPROVALS

Name	Company	Signature	Date
Mubarik Mustafa (Project Director)	ACET Solutions		
Abdulhadi G. Alshammari (Project Manager)	NWC		
Ahmed I. Almutairi (Project Sponsor)	NWC		

REVISION HISTORY

Rev No.	Date	Author	Checked By	Approved By	Comments
0	11-Feb-2021	AR	NR/SK	MM	Issued For Approval
1	11-Aug-2021	AR	NR/SK	MM	Issued For Approval

GLOSSARY

Acronyms	Meaning
WSUS	Window Server Update Services
SSL	Secure Socket Layer
ATM	Advance System and Technology
BU	Business Unit
DLD	Detailed-Level Design
DMZ	Demilitarized Zone
ECC	Essential Cybersecurity Controls
GB	Giga Byte
HCIS	High Commission for Industrial Security
HDD	Hard Disk Drive
HLD	High Level Design
HSE	Health, Safety, And Environmental
ICS	Industrial Control System
ISA	International Society of Automation
IT	Information Technology
JCBU	Jeddah Central Business Unit
KSA	Kingdom of Saudi Arabia
MCBU	Makkah Central Business Unit
MDCBU	Madinah Central Business Unit
MGMT	Management
NCA	National Cybersecurity Authority
NERC	North American Electric Reliability Corporation
NIST	U.S. National Institute of Standards and Technology
NWC	National Water Company
OT	Operational Technology
PDC	Primary Domain Controller
PS	Pumping Station
SCADA	Supervisory Control and Data Acquisition
TCP	Transmission Control Protocol
VM	Virtual Machine

REFERENCE DOCUMENTS

S/N	Document No.	Title
1	A01001045-HLD.00	High Level Design
2	ECC – 1: 2018	KSA NCA Essential Cybersecurity Controls (ECC – 1: 2018)
3	ISA–62443-1-1 (99.01.01)–2007	Security for Industrial Automation and Control Systems Part 1-1: Terminology, Concepts, and Models
4	A01001045-INV.00	NWC SCADA Asset Inventory
5	WSUS Patch Management	Microsoft WSUS Best Practices Guide
6	A01001045-DLD-PM-App1	Appendix A

Table of Contents

List of Figures:

1. DOCUMENT PURPOSE

This document aims to describe the detailed design of patch management for OT environment at NWC.

2. DESIGN PHILOSOPHY

The NWC Patch Management design is based on a hierarchical model. Patch Management Solution for NWC SCADA system is performed using Microsoft Window Server Update Services (WSUS).

3. DETAILED DESIGN

The section & its subsections describe the different elements of the Patch Management Design. A tiered based WSUS Servers Hierarchical Model is used to perform Patch Management.

3.1 WSUS ARCHITECTURE

The below figure shows the WSUS Patch Management Architecture for NWC SCADA/OT Environment:

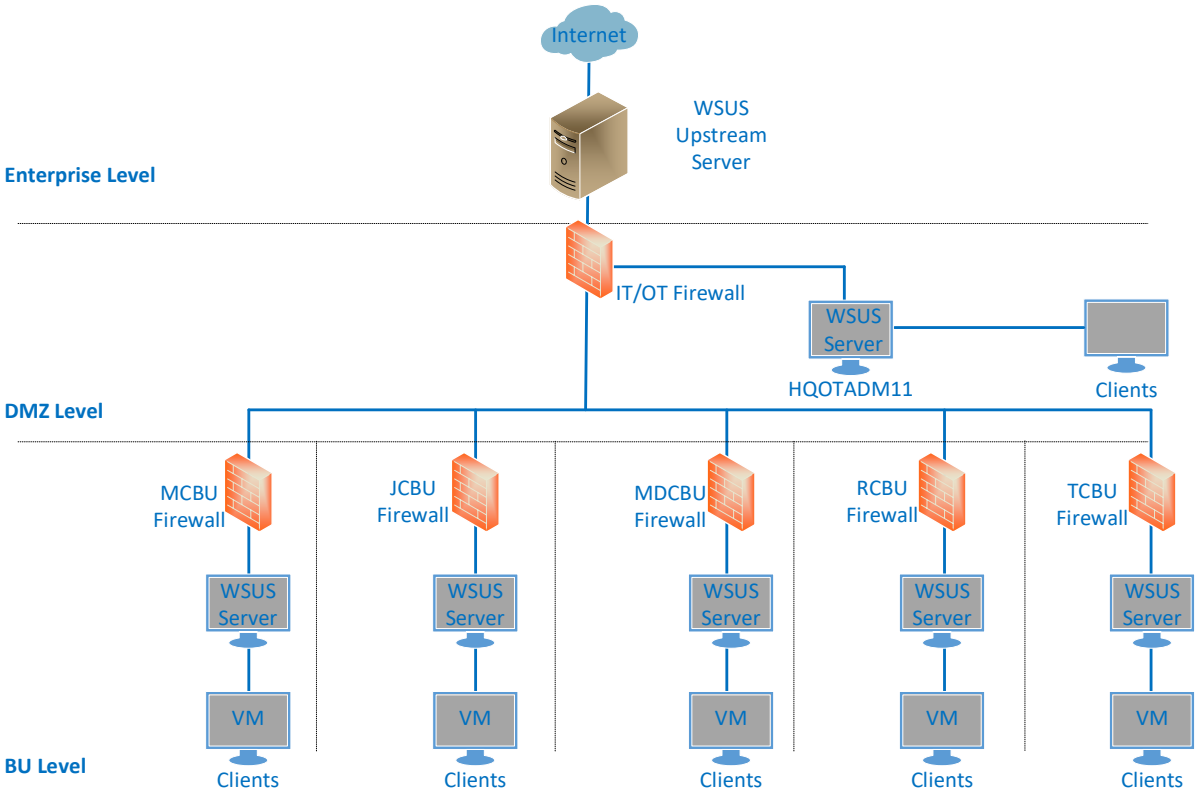

Figure 1: WSUS Architecture

- It is a tiered based design where an upstream IT WSUS server at NWC IT Level, OT WSUS Server at HQ OT DMZ Level, and OT WSUS Server at each BU.
- The IT WSUS Server at the NWC IT Level is configured to get updates from Microsoft Update Catalog Server through the internet
- IT WSUS shares updates with OT WSUS Server in HQ OT DMZ
- Each OT WSUS server at every BU manually synchronizes updates from HQ OT DMZ WSUS server.
- Workstations/Servers in MCBU (i.e., Awali, Mina, PS5, and Moassam/MAPA) are configured to get updates and patches from BU OT WSUS server at MCBU Main Office (i.e., at Awali).
- Workstations/Servers in RCBU sites are configured to get updates and patches from BU OT WSUS server at RCBU Main Office (i.e., at Exit-10).

3.2 WSUS CONFIGURATION

3.2.1 IT WSUS SERVER

The IT WSUS server at IT Level is configured to get updates from “Microsoft” and replicate it to an OT WSUS server in OT-DMZ.

Updates are stored locally on the IT WSUS server.

WSUS offers the ability to choose only the updates to require during synchronization. Synchronization is limited by language, product, and type of update.

Find attached the excel worksheet for products being downloaded from the Microsoft update catalog server to the WSUS upstream server.

3.2.2 OT WSUS SERVER AT OT-DMZ

OT WSUS server in OT-DMZ is distributing updates to all OT WSUS Server in each BU.

Following table list details of the OT WSUS Server VM at HQ OT DMZ:

Component	Requirements
VM name	HQOTADM11
Processor	6 cores
HDD-1	100 GB
HDD-2	800 GB
Memory	12 GB

Table 1: OT WSUS OT-DMZ Server

- On the OT WSUS server, a connection is created via port 8530 to pull the updates available in IT WSUS server at IT Level.
- OT DMZ Administrator manually downloads the patches and updates from IT WSUS to the OT WSUS server at HQ.
- These patches are manually validated by the HQ OT Administrator according to the Patch Management Procedures, Vendor(s) patch validation procedures (i.e. Patch

update validation & approvals from SCADA vendors) and then same are replicated to all the BU OT WSUS servers.

- Once approved the patches and updates are deployed on the all computers in OT-DMZ.

3.2.3 OT WSUS SERVER AT MCBU

Following table list details of the OT WSUS Server VM at MCBU:

Component	Requirements
VM	MAOTAWADM02
Processor	6 cores
HDD-1	80 GB
HDD-2	1.8 TB
Memory	12 GB

Table 2: OT WSUS Server at MCBU

- On OT WSUS server at MCBU, a connection is created via port 8530 to pull the updates available in OT WSUS server at OT-DMZ.
- OT MCBU Administrator manually downloads the patches and updates from OT WSUS server at HQ to the BU OT WSUS server.
- These patches are manually validated by the OT MCBU Administrator according to the Patch Management Procedures, Vendor(s) patch validation procedures (i.e. Patch update validation & approvals from SCADA vendors).
- Once approved the patches and updates are deployed on the all-client computers.
- All the clients in MCBU are configured through GPO to get updates from OT WSUS server at Awali.

Refer to A01001045-DLD-PM-App1.00 for scheduled detail:

3.2.4 OT WSUS SERVER AT RCBU

Following table list details of the OT WSUS Server VM at BU:

Component	Configurations
VM Name	RDOTE10ADM02
Processor	6
HDD-1	80
HDD-2	1.8 TB
D Drive (For Data)	1.9 TB
Memory	12 GB

Table 32: OT WSUS Server at RCBU

- On OT WSUS server at RCBU, a connection is created via port 8530 to pull the updates available in OT WSUS server at OT-DMZ.
- OT RCBU Administrator manually downloads the patches and updates from OT WSUS server at HQ to the BU OT WSUS server.

- These patches are manually validated by the OT RCBU Administrator according to the Patch Management Procedures, Vendor(s) patch validation procedures (i.e. Patch update validation & approvals from SCADA vendors).
- Once approved the patches and updates are deployed on the all-client computers.
- All the clients in RCBU are configured through GPO to get updates from OT WSUS server at Exit-10.

3.3 COMPUTER GROUPS

3.3.1 HQ COMPUTER GROUPS

Below drawing reflects the grouping of clients in NWC HQ:

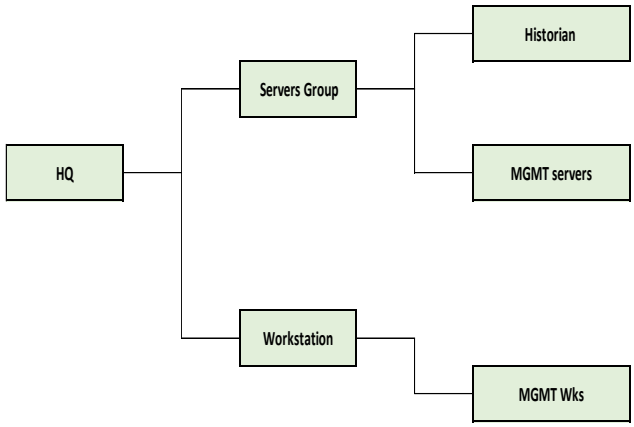

Figure 2: HQ Group Architecture

- All the clients are placed in their respective groups.
- Updates are applied according to group classification.
- Refer to excel file for different types of updates and how often they are applied to clients.

3.3.2 MCBU COMPUTER GROUPS

Below drawing reflects the grouping of clients in MCBU:

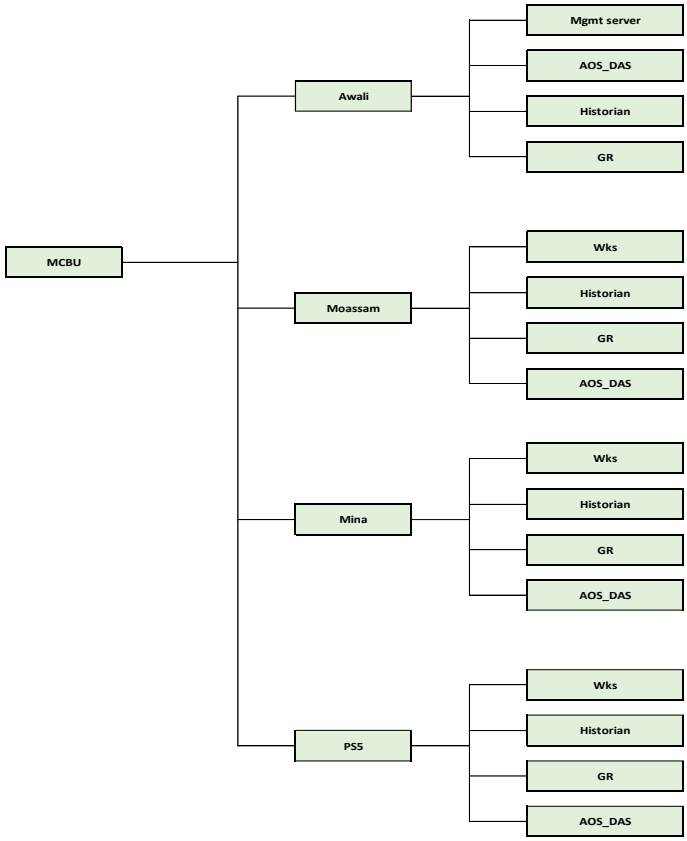

Figure 3: MCBU Group Architecture

3.3.3 RCBU COMPUTER GROUPS

Below drawing reflects the grouping of clients in some RCBU sites:

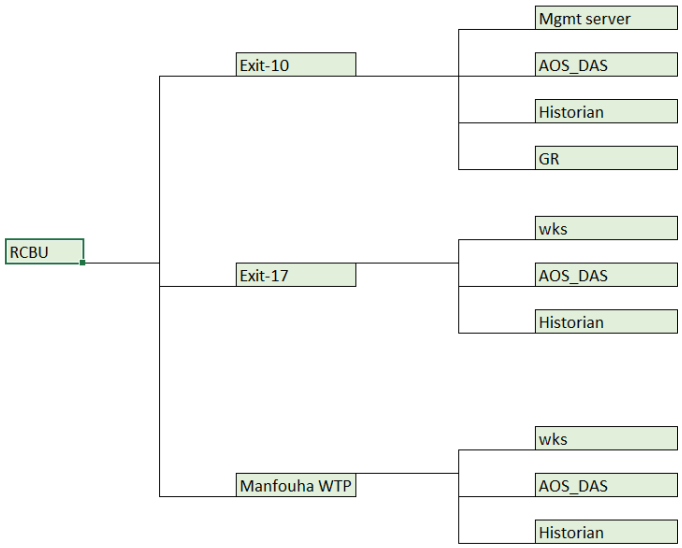

Figure 4 : RCBU Group Architecture of Some sites

- Groups are created for Bowaib WTP, Malaz WTP, Hayer WTP, Shomaisy WTP, Salbukh WTP, Wasi WTP, Manfouha WWTP, Heet WWTP, Hayer WWTP, TGW, TGC, TGNW, HPT, TGN, SR02.
- Clients are added to their respective groups and patches are applied according to schedule.
- Refer to excel file for different types of updates and how often they are applied to client.
- Patches are first approved by OT administrators and then pushed to all the clients on requirement basis.

3.4 PORTS REQUIREMENT

Review this table for details about port assignments.

3.4.1 SERVER TO SERVER COMMUNICATION

Port	Default Value	Description
Server-server SSL communication port	8531	Used to pull Updates

Table 43: Server-Server Communication Ports

3.4.2 CLIENT SERVER COMMUNICATION PORTS

Port	Default Value	Description
Client-server communication port	8530,8531	TCP port that the WSUS server uses to receive requests from clients.

Table 54: Client-Server Communication

Refer to A01001045-DLD-PM-App1.01 for scheduled detail:

ACET Solutions LLC
1400 Broadfield Blvd Suite 200 Houston TX, 77084.
United States of America.
Tel: +1 832 386 5593 | Fax: +1 832 201 0337
sales@acetsolutions.com | www.acetsolutions.com