NWC OT Cybersecurity Active Directory Detailed Design

National Water Company (NWC), KSA

SCADA/OT Information Security Implementation Project

Document Number:	A01001045-DLD-AD
Document Title:	NWC OT Cybersecurity Active Directory Detailed Design
Document Version:	01
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
ACL	Access Control Lists
AD	Active Directory
ADC	Additional Domain Controller
ATM	Advance System and Technology
ATP	Adaptive Threat Protection
BOM	Bill of Material
BU	Business Unit
BYOD	Bring Your Own Device
CAP	Client Authorization Policy
CAS	Central Administration Server
CIP	Critical Infrastructure Protection
CMC	Central Management Console (Nozomi)
CSMS	Cyber Security Management System
DCS	Distributed Control System
DMZ	Demilitarized Zone
DNS	Domain Name System
DNS	Domain Name System
ECC	Essential Cybersecurity Controls
ePO	ePolicy Orchestrator
EPP	End Point Protection
GPS	Global Positioning System
HCIS	High Commission for Industrial Security
HLD	High Level Design
HMI	Human Machine Interface
HSE	Health, Safety, And Environmental
ICS	Industrial Control System
IDS	Intrusion detection System
IPS	Intrusion Prevention System
ISA	International Society of Automation
ISO	International Organization for Standardization
IT	Information Technology
JCBU	Jeddah Central Business Unit
KSA	Kingdom of Saudi Arabia
MBSS	Minimum Baseline Security Standards
MCBU	Makkah Central Business Unit
MDCBU	Madinah Central Business Unit
MGMT	Management
NCA	National Cybersecurity Authority
NERC	North American Electric Reliability Corporation
NGFW	Next Generation Firewall
NIST	U.S. National Institute of Standards and Technology

NTP	Network Time Protocol
NWC	National Water Company
OT	Operational Technology
PDC	Primary Domain Controller
PLC	Programmable Logic Controller
RAP	Resource Authorization Policy
RCBU	Riyadh Central Business Unit
RD	Remote Desktop
RDS	Remote Desktop Services
RTO	Recovery Time Objective
RPO	Recovery Point Objective
SCADA	Supervisory Control and Data Acquisition
SIEM	Security Incident & Event Management Solution
SSL	Secure Socket Layer
TCBU	Taif Central Business Unit
VLAN	Virtual Local Area Network
VM	Virtual Machine
OU	Organizational Unit

REFERENCE DOCUMENTS

S/N	Document No.	Title
1	A01001045-HLD	High-Level Design
	A01001045-DLD-AD-App1.00	Active Directory details Appendix
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

Table of Contents

List of Figures

List of Tables

1. DOCUMENT PURPOSE

The purpose of this document is to describe the detailed-level documentation of active directory infrastructure for OT environment at NWC. This document contains general data followed in NWC for active directory deployment and provides a broad overview of the whole environment.

2. DESIGN

2.1 ACTIVE DIRECTORY

Every object in Active Directory is an instance of a class defined in the schema. Each class has attributes that ensure each object's Unique identification (instance of a class) in a directory data store. The following sections contain the name of the domain.

- The AD forest name is the NWC-OT.
- The active directory domain name is the abridged version of the organization's name anteceded by the letter LOCAL i.e., NWC-OT.LOCAL.

The Active Directory database file (Ntds.dit), log files, and SYSVOL files are stored on a separate virtual disk from the operating system files.

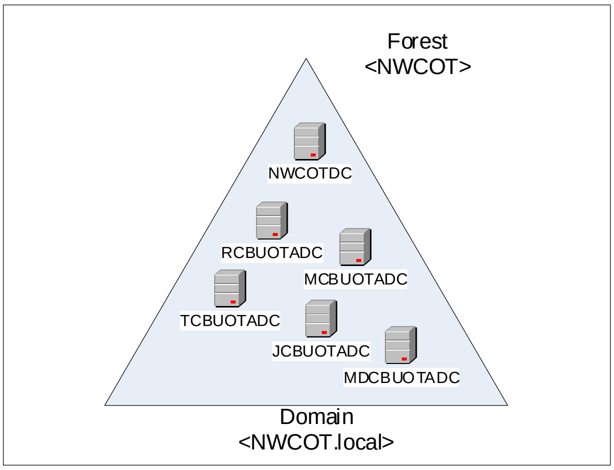

Figure 1: Active Directory Structure

2.2 DOMAIN CONTROLLER PLACEMENT

Forest root DC is needed to create Active Directory trust paths for clients who need to access resources and the FMSO roles.

The following table contains the forest root DC summary information.

Root DC Summary	
Root domain controller	HQOTADM01
Physical Location	NWC-HQ
FSMO roles	Enable
Global Catalog	Enable
DNS roles	Yes

Table 1: Root DC Summary

2.3 ADDITIONAL DOMAIN CONTROLLER PLACEMENT

Additional DCs will be placed in every BU main office. ADC in MCBU is configured as:

Additional DC Summary	
Additional domain controller	MAOTAWADM01
Physical Location	MCBU-Awali
FSMO roles	Enable
Global Catalog	Enable
DNS roles	Yes

Table 2: MCBU Additional Domain Controller Summary

ADC in RCBU is configured as:

Additional DC Summary	
Additional domain controller	RDOTE10ADM01
Physical Location	RCBU Exit-10
FSMO roles	Enable
Global Catalog	Enable
DNS roles	Yes

Table 3: RCBU Additional Domain Controller Summary

2.4 ORGANIZATIONAL UNITS (OUS) DESIGN

OUs are Active Directory (AD) containers that hold other AD objects.

It has three main functions:

- To visually organize objects.
- To group objects so Group Policies can be assigned to them.
- To group objects so permissions can be delegated to them so they can be managed by a subset of administrators.

2.4.1 ORGANIZATION UNITS

Organizational units (OU's) are created, and objects are added to their respective OU's having similar profiles.

The following list of OUs and Security Groups are created:

Computer OUs	OU Description
C_MGMT	OU for All Management Servers, it includes AVP Servers, Backup Servers, WSUS Servers, SFTP Servers, Syslog Servers & etc.
C_OWS	OU for All SCADA Operator Workstations
C_EWS	OU for All SCADA Engineering Workstations
C_SCADASVRs	OU for All SCADA Servers
C_StandAlone	OU for All SCADA Standalone Laptops/Workstations (those stations that are frequently used for field device configurations)

Table 4: Computer OUs

Users OUs	OU Description
U_Admins	User OU for Domain Administrator & SCADA Administrators
U_Operators	User OU for SCADA Operators
U_ApplicationEngineers	User OU for SCADA Application Engineers
U_USBUsers	User OU for all Users having USB Access Permission
U_SystemEngineers	User OU for Systems Engineers, it includes all users having permissions to modify Computer Systems Settings
U_Service Accounts	User OU for Service Accounts

Table 5: Users OUs

2.4.2 User Security Groups

The following list of User Security Groups are created, this is to simplify and establish consistency on user rights assignment & permissions.

Users Security Group	Security Group Description
U_Admins	User Group for Domain Administrator & SCADA Administrators
U_Operators	User Group for SCADA Operators
U_ApplicationEngineers	User Group for SCADA Application Engineers
U_USBUsers	User Group for all Users having USB Access Permission
U_SystemEngineers	User Group for Systems Engineers, it includes all users having permissions to modify Computer Systems Settings
U_Service Accounts	User Group for Service Accounts

Table 6: User Security Groups

2.5 CLIENT-SIDE CONFIGURATION AND SETTINGS

The purpose of Active Directory Client is to enable the client machine to access information stored in Active Directory on domain controllers in the network.

Before joining the domain, each client must have:

- For clients in NWC HQ the primary DNS is pointing towards the root domain controller.
- For clients in each BU, primary DNS is pointing towards ADC in their respective BU, and secondary DNS is pointing towards root domain Controller.
- Clients are moved to their respective OU after joining domain.

2.6 GROUP POLICIES (GPO'S)

Group Policy Objects are used to centrally manage the security and configuration of Domain computers/users in AD DS.

Computers/Users with similar functions are utilizing same GPO for the computer function, thereby ensuring compliance, consistency, and standardization.

Where multiple GPOs are linked to a particular object, GPOs precedence will be set; by default, the last applied configured setting is used.

The following list of Group Policies are created (for details about each GPO, please refer to document "A01001045-DLD-AD-App1.01").

OU	Linked GPOs
NWC	C_NWC Default Computers Policy_GP
NWC	U_ NWC Default Users Policy _GP

Computer OUs	Linked GPOs
C_MGMT	C_MGMT_GP
C_OWS	C_OWS_GP
C_EWS	C_EWS_GP
C_SCADASVRs	C_SCADASVRs_GP
C_Standalone	C_Standalone_GP

Table 7: Group Policies applied to Computer OUs

User Groups	Linked GPOs
U_Admins	U_Admins_GP
U_Operators	U_Operators_GP
U_ApplicationEngineers	U_ApplicationEngineers_GP
U_USBUsers	U_USBUsers_GP
U_SystemEngineers	U_SystemEngineers_GP

Table 8: Group Policies applied to User OUs

2.7 AD FIREWALL PORTS

The following table represents ports that are enabled:

Protocol and Port	Description	Type of Traffic
TCP 25	Replication	SMTP
TCP 42	NetBIOS resolution	WINS
TCP 135	Replication	RPC, EPM
TCP 137	NetBIOS Name resolution	NetBIOS Name resolution
TCP 139	User and Computer Authentication, Replication	DFSN, NetBIOS Session Service, NetLogon
TCP and UDP 389	Directory, Replication, User and Computer Authentication, Group Policy, Trusts	LDAP
TCP 636	Directory, Replication, User and Computer Authentication, Group Policy, Trusts	LDAP SSL
TCP 3268	Directory, Replication, User and Computer Authentication, Group Policy, Trusts	LDAP GC
TCP 3269	Directory, Replication, User and Computer Authentication, Group Policy, Trusts	LDAP GC SSL
TCP and UDP 88	User and Computer Authentication, Forest Level Trusts	Kerberos
TCP and UDP 53	User and Computer Authentication, Name Resolution, Trusts	DNS
TCP and UDP 445	Replication, User and Computer Authentication, Group Policy, Trusts	SMB, CIFS, SMB2, DFSN, LSARPC, NbtSS, NetLogonR, SamR, SrvSvc
TCP 9389	AD DS Web Services	SOAP
TCP 5722	File Replication	RPC, DFSR (SYSVOL)
TCP and UDP 464	Replication, User and Computer Authentication, Trusts	Kerberos change/set password
UDP 123	Windows Time, Trusts	Windows Time
UDP 137	User and Computer Authentication	NetLogon, NetBIOS Name Resolution
UDP 138	DFS, Group Policy, NetBIOS Netlogon, Browsing	DFSN, NetLogon, NetBIOS Datagram Service

Table 9: Firewall Ports

3. DNS DESIGN

Domain Controllers (DC) and all Additional Domain Controllers (ADC) are configured as DNS Server.

Function	Settings
DNS	Secure DNS dynamic registration is configured. Reverse lookup zones are configured. DNS forwarding is not configured. DNS Aging and Scavenging is disabled (standard values)

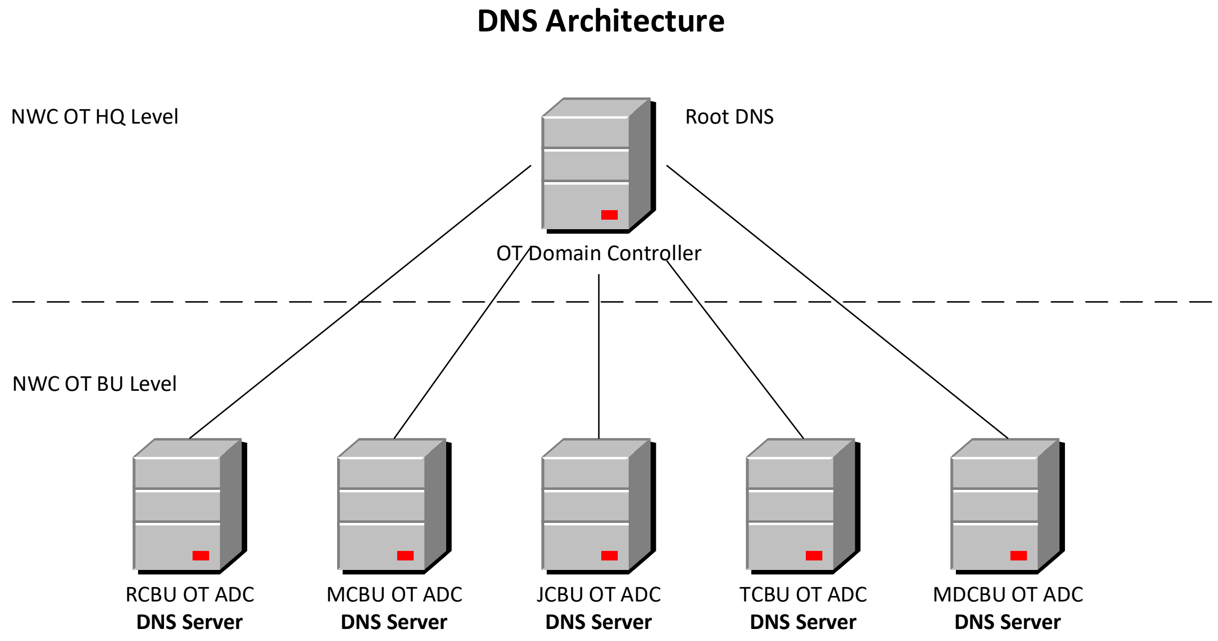

Figure 2: DNS Architecture

3.1 DNS INFRASTRUCTURE SETTINGS

The DNS Server is configured using the following settings:

Tab	Settings	Configurations
Interface	Use of interface	Listen on the specific IP address for DNS requests
No Forwarders	Forwarders will not be configured	No Forwarders
Advanced	Server options	Disable recursion = checked Bind secondaries = unchecked Fail on load if bad zone data = unchecked Enable round robin = checked Enable netmask ordering = checked Secure cache against pollution = checked
Root Hints	no Root Hints	By configuring the root DNS server Root hints will be cleared
Event Logging	Event logging	Log all Events

Debug Logging	Debug Logging	keep Disabled
	DNS Events: Log size	Log size = 20 MB
	DNS Events: Log retention	Logfile retention = Overwrite events as needed
Monitoring	Do not perform automatic testing	Keep perform automatic testing disabled
Security	Leave default	Do not modify defaults

Table 10: DNS Settings

4. TIME SYNCHRONIZATION

GPS Clock and Master NTP Server will be installed at NWC HQ and will serve as Time Master to all domain clients.

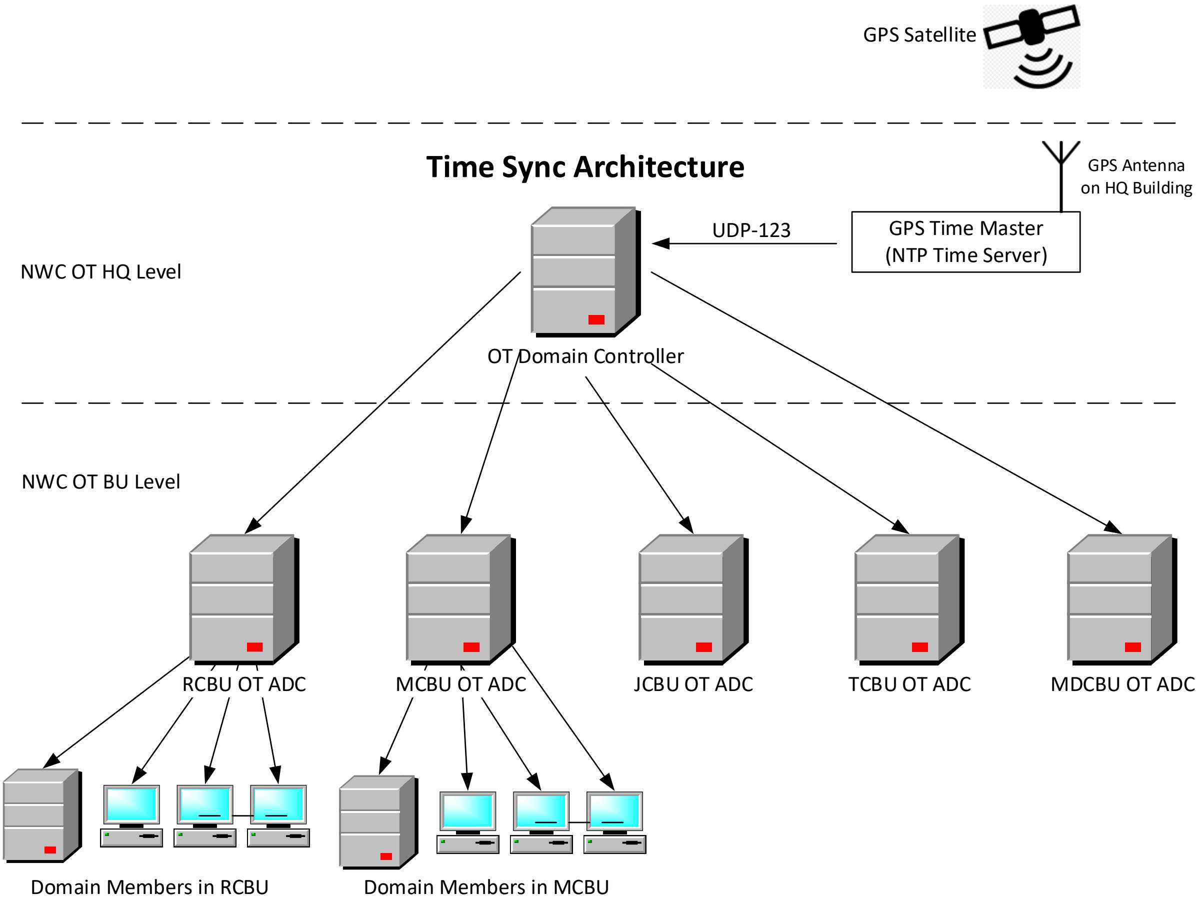

Figure 3: Time Synchronization

4.1 TIME CONFIGURATION

Item	Settings
Time Zone	GMT + 3(Saudi Arabia)
Automatically adjust for daylight saving	Disable

Table 11: Time Configuration

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