NWC OT Cybersecurity Remote Access Management Detailed-Level Design

National Water Company (NWC), KSA

SCADA/OT Information Security Implementation Project

Document Number:	A01001045-DLD-RA
Document Title:	NWC OT Cybersecurity Remote Access Management Detailed-Level Design
Document Version:	0
NWC Contract No.:	101200487
[atm] PO Ref.:	ATMPO2020-034

NOTES AND COPYRIGHTS

The information contained in this document is confidential, privileged, and only for the intended recipient's information and may not be used, published, or redistributed without the prior written consent of ACET Solutions LLC. This document contains confidential, sensitive information of National Water Company (NWC).

Information contained herein is for the sole use of the customer (NWC) receiving this document. Acceptance of the document by the customer constitutes agreement by the customer & ACET Solutions that either party shall not disclose confidential information to any third party and shall not transmit any documents or copies thereof containing confidential information to any third party except as may by authorized in writing by NWC & ACET Solutions.

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

GLOSSARY

Acronyms	Meaning
AD	Active Directory
ADC	Additional Domain Controller
ATM	Advance System and Technology
ATP	Adaptive Threat Protection
BU	Business Unit
DLD	Detailed-Level Design
DMZ	Demilitarized Zone
RD	Remote Desktop
RD CAP	Remote Desktop Client Authorization Policy
RD RAP	Remote Desktop Resource Authorization Policy
ECC	Essential Cybersecurity Controls
GB	Giga Byte
HCIS	High Commission for Industrial Security
HDD	Hard Disk Drive
HLD	High Level Design
HMI	Human Machine Interface
HTTP	Hypertext Transfer Protocol
HSE	Health, Safety, And Environmental
ICS	Industrial Control System
IDS	Intrusion detection System
IPS	Intrusion Prevention 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	NWC OT Cybersecurity 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	RDS Infrastructure	Microsoft Remote Desktop Services Documentation

Table of Contents

List of Tables

1. DOCUMENT PURPOSE

The purpose of this document is to describe the detailed design of remote access management for the OT environment at NWC.

2. DESIGN PHILOSOPHY

Remote access management for NWC SCADA system is performed using Microsoft Windows remote desktop services (RDS) using RD gateway. The purpose of using is RD Gateway services is to monitor and manage Remote desktop connection within OT Network; no connection from IT or Internet to RD Gateway is allowed.

3. DETAILED DESIGN

Remote Desktop Services is a technology that allows the client to establish remote sessions to system resources.

- The Remote Desktop Gateway (RD Gateway) role service provides access to authorized remote users to any system resources using secure and encrypted connections.
- The RD-Gateway is integrated with a primary domain controller to manage remote access for all devices and users within the OT domain.
- An RD-Gateway server deployed in OT-Domain Zone provides central management and control of remote access.
- RD licensing server is deployed in OT-Domain Zone, and client access license (RDS CAL) is configured for all client devices to access system resources.
- The licensing server is configured in “per user” mode.
- RD session host, Connection broker RD web access and RD gateway server in OT-Domain zone is deployed on HQOTADM12.
- A self-signed certificate is configured for both RD gateway server and RD licensing server and this certificate is added to trusted root certificate authority store in each client machine.

3.1 RD GATEWAY SERVER CONFIGURATION

RD gateway server in OT-Domain zone has the following configurations:

Component	Configuration
VM name	HQOTADM12
Processor	6 cores
HDD-1	100 GB
HDD-2	100 GB
Memory	12 GB

Table 1: RD Gateway Server Configuration

3.2 CONNECTION AUTHORIZATION POLICIES

RD Gateway server uses connection authorization policies (RD CAPs) to specify users connect through the RD Gateway server to system resources.

- A remote desktop users' group is created in AD, only this group is allowed to access system resources through RD CAP configuration.
- Remote desktop users who are frequently using RD services are added to remote desktop user group so they are able to access machines remotely.
- Remote users in same BU are not allowed to create remote session in other BU.
- Remote desktop user group created in HQ is allowed to access machines remotely in each BU.

3.3 RESOURCE AUTHORIZATION POLICIES

RD Gateway uses resource authorization policies (RD RAPs) to determine the specific resources that an incoming RD Gateway client is able to use.

- A remote desktop computer group is created in AD and all the computers used for remote services are added to that group.
- The remote desktop computer group is accessible to remote users through RD RAP configuration.

3.4 PORTS REQUIREMENT

Review this table for details about port assignments.

Port	Default Value	Description
For authentication of usres	88	TCP port 88 for Kerberos.
RPC Endpoint Mapper	135	This communication provides the TCP port for communicating with the NTDS RPC service for AD DS
RD communication	3389	TCP port RDP Traffic for communicating with RD Session Hosts
RADIUS and RADIUS accounting	1812,1813	UDP ports for RADIUS traffic
SSL	443	Secure communication for from client to RD server

Table: Ports Requirement

ACET
SOLUTIONS

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