NWC OT Cybersecurity Backup Management Detailed Design

National Water Company (NWC), KSA

SCADA/OT Information Security Implementation Project

Document Number: A01001045-DLD-BM
Document Title: NWC OT Cybersecurity Backup Management Detailed-Level Design
Document Version: 01
NWC Contract No.:   101200487
[atm] PO Ref.:   ATMPO2020-034

NOTES AND COPYRIGHTS

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	HH	NR/SK	MM	Issued For Approval
1	11-Aug-2021	AR	NR/SK	MM	Issued For Approval

GLOSSARY

Acronyms	Meaning
AD	Active Directory
ATM	Advance System and Technology
BU	Business Unit
CAP	Client Authorization Policy
CAS	Central Administration Server
CSMS	Cyber Security Management System
DMZ	Demilitarized Zone
ECC	Essential Cybersecurity Controls
HCIS	High Commission for Industrial Security
HLD	High Level Design
HSE	Health, Safety, And Environmental
ICS	Industrial Control System
ISA	International Society of Automation
IT	Information Technology
KSA	Kingdom of Saudi Arabia
MCBU	Makkah 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
RTO	Recovery Time Objective
RPO	Recovery Point Objective
SCADA	Supervisory Control and Data Acquisition
VM	Virtual Machine

REFERENCE DOCUMENTS

S/N	Document No.	Title
1	A01001045-HLD.00	NWC OT Cybersecurity High-Level Design
2	A01001045-INV.00	NWC SCADA Asset Inventory
3	A01001045-DLD-BM-APP1.00	Backup Plan
3	ECC – 1: 2018	KSA NCA Essential Cybersecurity Controls (ECC – 1: 2018)
4	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

This document serves as a detailed design for the Backup Solution of the NWC SCADA. It lists all the installations and configurations required to implement the Backup solution using the Veritas BackupExec software solution in a tiered structure.

2. BACKUP DESIGN ARCHITECTURE

The following diagram illustrates the tier-based Backup solution design of the NWC SCADA where there is a Central Administration Server (CAS) at the HQ OT-DMZ, and managed backup servers at each BU Main Office SCADA zone.
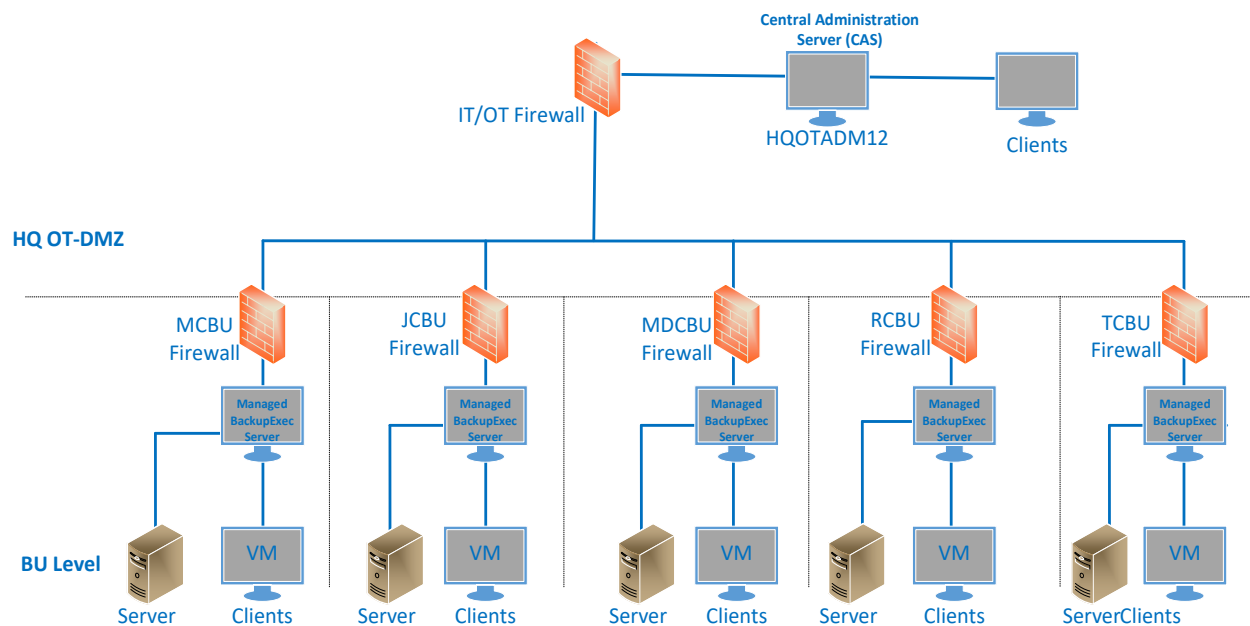

Figure 1: NWC Backup Architecture

3. BACKUP MANAGEMENT DESIGN

Veritas BackupExec Gold edition is being installed and configured in the NWC-SCADA. The following sections explain the detailed design. All backups will be stored locally on the BU/HQ backup server as per backup plans.

3.1 CENTRAL ADMINISTRATION SERVER (CAS)

The Veritas BackupExec CAS is the central backup management server for the NWC SCADA. It monitors and manages all the Managed BackupExec servers in the BU Main offices as well as its own clients. It is managed using the service account "Svc-backup", which is part of the "backup Operators" group in the Active Directory.

The storage space allocated to backups for the CAS is 2 TB. Backups will be stored locally on the HDD-2 of the same server.

Following are the system configurations for the installation of Veritas BackupExec CAS server

Component	Configurations
VM name	HQOTADM12
CPU Cores	6
O/S	Microsoft Windows Server 2019 Standard
C Drive (For VM O/S)	100 GB
D Drive (For Data)	3 TB
Memory	12 GB
Software Installed	BackupExec-CAS, SFTP, Qradar SF

Table 1: CAS configuration

3.1.1 CAS INSTALLATION CONFIGURATION

CAS installation features:

- Agent for VMware and Hyper-V

- Deduplication Feature

- Online Documentation

- Agent for Applications and Databases

- Advanced Disk-based Backup Feature

- Central Admin Server feature

3.2 MANAGED BACKUPEXEC SERVER

The Veritas Managed BackupExec servers are the local BU level backup management servers and are centrally managed by the CAS. These servers manage their respective BU sub-sites as well as their own clients.

The storage space allocated to backups for the Managed BackupExec server is 1 TB. Backups will be stored locally on the HDD-2 of the same server.

Following are the system configurations for the installation of Veritas Managed BackupExec server at MCBU

Component	Configurations
VM name	MAOTAWADM02
CPU Cores	6
O/S	Microsoft Windows Server 2016 Standard
C Drive (For VM O/S)	100 GB
D Drive (For Data)	1.8 TB
Memory	12 GB
Software Installed	WSUS,BackupExec-MG, SuperAgent(McAfee)

Table 2: MCBU Managed BackupExec server configurations

Following are the system configurations for the installation of Veritas Managed BackupExec server at RCBU

Component	Configurations
VM name	RDOTE10ADM02

Component	Configurations
CPU Cores	6
O/S	Microsoft Windows Server 2016 Standard
C Drive (For VM O/S)	100 GB
D Drive (For Data)	1.8 TB
Memory	12 GB
Software Installed	WSUS,BackupExec-MG, SuperAgent(McAfee)

Table 3: RCBU Managed BackupExec server configurations

3.2.1 MANAGED BACKUP SERVER INSTALLATION CONFIGURATION

Managed Backup Exec server installation features:

- Agent for VMware and Hyper-V

- Deduplication Feature

- Online Documentation

- Agent for Applications and Databases

- Advanced Disk-based Backup Feature

- Managed Backup Exec feature

3.3 BACKUPEXEC SERVICES & PORTS

Following services and their respective ports are utilized by Veritas BackupExec-

Service	Process	Port	Port Type
Backup Exec Agent Browser	benetns.exe	6101	TCP
Device and Media Service	pvlsvr.exe	None	None
Backup Exec Server	beserver.exe	3527, 6106	TCP
Backup Exec Job Engine	bengine.exe	5633 by default Can be customized	TCP
Agent for Windows Agent for Linux Agent for Oracle on Windows or Linux	Beremote	10000 Dynamic range between 1024 to 65535 by default Can be customized	TCP
Alert Server	alertserver.exe	None	None
Backup Exec Management Service	BackupExecManagementService.exe	50104	TCP
Deduplication engine	Spoold.exe	10082	TCP
Deduplication Manager	Spad.exe	10102	TCP

Table 4: BackupExec Services & Ports

3.4 BACKUP PLAN

Refer to document "A01001045-DLD-BM-APP1.01" for details of backup plan including backup frequency, scheme, and retention.