VCL-9090
NAS Data Storage
with Cyber Security

ORION TELECOM NETWORKS

Product Overview

The VCL-9090 is a powerful, Industrial-grade Network Attached Storage (NAS) Server that is designed for businesses and organizations that require high-performance storage, select data sharing, and quick retrieval of large-scale data. The VCL-9090, when installed in the **Orion Data-storage (ODE) Eco-system** provides not only a fault-tolerant, high dependability, high-reliability data storage solution but also offers a high resilience to internal faults as well as to external threats, such as ransomware attacks. The VCL-9090 can store up to 60 (HDD) drives, each with a maximum capacity of up to 20 TB giving a raw data storage capacity of more than 1 PB (i.e., more than 1000 TB). The VCL-9090, offers unique features that alerts network administrators, in real-time, in case of any alarms (such as arising from impending disk failures, possible hostile network intrusions, or a possible ransomware attack).

The server also provides hard disk access on a per interface basis so that any disk (or a set of disks) can be dedicated to a particular department which can only be accessed by those select entities thereby improving security and data management. The VCL-9090 supports various RAID configurations for improved redundancy and performance. The Industrial-grade NAS server comes with redundant power supplies, hot-swappable drives in a rugged industrial chassis, making it suitable for installation in data centres where data integrity and data security is of utmost importance.

Administrators can securely manage and monitor the VCL-9090 through its NMS, which is an intuitive, web-based interface. In summary, the Industrial-grade NAS server is an ideal storage solution for businesses and organizations that are seeking reliable and scalable storage infrastructure with advanced features and a robust design.

Available RAID configuration

No. of Drives	24
Size of each Drive	20 TB or higher
RAW Data Capacity	480 TB

RAID level	Capacity after RAID (for 24 Drives)	Fault Tolerance
RAID 0	480 TB	0 Drive per RAID set
RAID 1	20 TB	23 Drives per RAID set
RAID Z1 (5)	460 TB	1 Drive per RAID set
RAID Z2 (6)	440 TB	2 Drives per RAID set
RAID Z3 (7)	420 TB	3 Drives per RAID set

Device Specific Information

Description	VCL-NAS
Maximum number of drives	60 (optional)
Physical Dimensions	D x W x H: 760 x 480 x 180mm
Net Weight	18.5 Kgs. (without HDD)
Weight of each HDD	0.6 Kgs. (maximum upto 60 HDD)
Redundant Power Supply	1+1, 800W Dual AC Power Supply

Highlights

- NAS server with up to 60 hard drives and maximum 20 TB per drive storage.
- 4 x Dry Contact external alarm relays which may be wired to external, multiple user-configurable audio and visual alarms, which shall include:
  - Ransomware detection alarm
  - Disk removal alarm
  - Disk failure alarm
  - High Temperature alert
  - Power Supply failure alarm
  - RAID degradation alarm
  - Disk S.M.A.R.T test failure alarm
  - Disk-Pool storage capacity usage alert
- Each audio / visual alarm can be assigned to a specific alarm.
- Restrict data access based on IP ranges, physical network connections or predefined network policies.
- Storage elements (i.e. data drives) can be assigned on a per-interface basis.
- Large capacity for storage makes it an ideal solution for government, businesses and research organizations.
- Vast amounts of data can be stored, including high-quality multimedia files, large datasets, and backups.
- Allows the administrator to assign specific storage elements to specific users so that a particular set of users are granted access to only those specific hard drives.
- The VCL-9090 is a reliable and scalable solution for users that require a scalable data storage solution based on their growing needs and requirements.
- Provides an added layer of security for data access.
- Secure, visual NMS. Allows the data administrator to securely manage the VCL-9090 through an intuitive management and monitoring interface with a 24x7 live view of all operational parameters.
- Prompt notifications of any issues allows the network administrators to take appropriate and timely actions to prevent data loss and mitigate ransomware attacks.
- Allows for customization and flexibility in terms of hardware and software components.
- Can store large amounts of data without compromising on speed or performance.
- Helps businesses and organizations manage their data more efficiently.
- Enables quick access to important files and data.
- Provides a centralized location for data storage.
- In addition to primary data storage, additional VCL-9090 data storage servers can be installed on-location and off-location to provide backup data storage. The concept of storing backup data both on-location and off-location helps greatly in mitigating loss of data due to natural or man-made disasters.
- Greatly reduces the risk of data loss due to hardware failure or other disaster related events.
- Allows for easy expansion of storage capacity as needed.
- Provides cost-effective solution for users in need of large-scale and reliable storage.
- Provides integration with 3rd party backup applications.
- Provides integration with Cloud.
- Allows more than 50% compression.
- Facilitates Replication from day one of installation.
- Facilitates Deduplication from day one of installation.

Key Cyber Security Features

- Ransomware resilient NAS & Data Storage solution
- Quantum-safe cryptography protection layer – Optional
- Multi-factor Authentication - TOTP (Time + OTP based)
- 2 Factor Authentication based SSH access
- Audio and Visual Alerts in the event of Disk removal/failure
- AI based Behavioural Analytics
- Lock-down of Local Console on Primary and Secondary NAS Systems to prevent un-authorized access
- Hardware Security Modules (HSMs)
  - Specialized hardware devices designed to securely store cryptographic keys and perform cryptographic operations.
  - HSMs are used in environments where high levels of security are essential, such as in financial services, government, utilities and large enterprises.
- Perpetual Licence at no extra cost
- Data Encryption - AES 256
- Physical Tamper Detection
- Network Management System-Extensive monitoring (HTTP(S) based)
- Encrypted Backup and Disaster Recovery
- On-site and Off-Site data backups
- Periodic, user scheduled, incremental data back up sessions of offsite system with active, hard network isolation
- Encryption key validation before Encrypting any data
- Audio/Visual Alarms in the event when an unvalidated / unauthorized encryption key is attempted to be used
- Recurring Read-only Snapshots
- Long Retention Time on Snapshots
  - Daily snapshots (2 weeks retention)
  - Weekly snapshots (1 year retention)
  - Monthly snapshots (5 years retention)
  - Annually snapshots (10 years retention)
- Snapshots with WORM Technology
- User programmable option to increase the Snapshot
- Retention Duration on the Destination System
- Replicate to a Secondary NAS System
- Using a Separate Replication Network
- Set Separate Administrative Passwords
- Configurable Two-Factor Authentication (2FA) for Administrators

Hardware Specifications

Processor	Intel Xeon
Number of Cores	32 Physical Cores
RAM	Upto 256 GB
Network Access Ports	- 4 x 1G Electrical Ethernet (RJ45) Ports - 4 x 1G Optical (SFP) Ports - 4 x 10G Optical (SFP+) Ports
Dedicated management Port	- 1 x 1G Ethernet Port
Additional Access Ports	- 2 x USB 3.2 (Minimum) - 1 x RS232 Console Port
Alarms and Display	- 4 x dry-contact alarms for connecting external, user assignable, audio-visual alarms. - 1 x 21-Inch (or greater) Display for configuration
Power Supply	- 1+1, Dual 220VAC, 50Hz, Hot-Swappable minimum 800W Redundant Power Supplies to support up to 60 data storage HDDs.
Operating Temperature	10C ~ 35C (50F ~ 95F)
Storage Temperature	-40C ~ 70C (104F ~ 158F)
Storage Humidity	20% ~ 90% (non-condensing)

Ransomware-Resilient Features

- **Data Access Patterns and Analysis:** Intelligent detection of Ransomware encryption activities incorporating continuous monitoring of files and activities to maintain a secure environment and prevent potential breaches.
- **Automated Threat Response:** Audio/visual alarms triggered upon Network Intrusion and Ransomware activity detection
- **Data Protection Mode:** The system automatically switches to a read-only mode to safeguard existing data from unauthorized modifications or encryption, ensuring data integrity.
- **Read-Only Snapshots:** The immutability of read-only files and folders provides a robust defence against Ransomware attacks by preventing their encryption.

Additional Security Features

- **“Pull Replication” in Offsite Server:** The offsite backup server autonomously initiates a network connection to facilitate a scheduled data backup and then automatically disconnect from the network after executing its periodic data backup.
- **NTP Synchronization for Scheduled Backup Service:** The offsite backup server synchronizes its operations with the on-site Network Time Protocol (NTP) Server, establishing connections at predetermined administrator assigned times and seamlessly going offline upon successful backup completion.
- **Resilience to Ransomware Attack via Read-Only Snapshots:** The immutability of read-only files and folders provides a robust defence against ransomware attacks by preventing their encryption
- **IP Filtering Capabilities:** Administrators have granular control over access permissions by specifying the allowed IP domains for specific shared resources
- **Network Access Protection:** Access to server resources and shares is restricted based on predefined IP address ranges, enhancing security and control
- Two-step authentication for secured access
- **HTTPS Secure Connection:** A secure Hypertext Transfer Protocol Secure (HTTPS) connection is established to protect the web-based graphical user interface (GUI) against potential Man-in-the-Middle (MITM) attacks.
- **Importable SSL Certificate Requirement:** The establishment of HTTPS connections necessitates the presence and utilization of SSL certificates for secure data transmission.
- **AES 256-bit Volume-Based Data Encryption:** Sensitive data may also selectively be safeguarded through implementation of advanced 256-bit AES encryption, applied at the volume level.

Regulatory Compliance:

- RoHS
- CE Marking
- Complies with FCC Part 68 and EMC FCC Part 15

Specifications subject to change for improved product performance and capacity.

Software Specifications

Operating System	UNIX based purpose built OS.
Licences	Software and license is included with the equipment at no additional cost or charge. There will be no recurring or additional bi-annual / or annual recurring licence payments that are required to be made after the purchase of the equipment. The included licence is for perpetual use during the lifetime of the NAS data storage server equipment that is being offered.
Protocols	iSCSI, CIFS/SMB, WebDAV, AFP, NFS, S.M.A.R.T., FTP, HTTP, HTTPS, SSH, LLDP, SNMP, SMTP
File System	- Internal: EXT3, EXT4 - External: NFS, CIFS, EXT3, EXT4, NTFS, FAT32
Networking	- TCP/IP IPv4 & IPv6 Dual Stack - Dual Gigabit Ethernet with Jumbo Frame - Multi-IP Setting, Port Trunking, Failover, 802.3ad - DHCP Client - UPnP & Bonjour Discovery - OpenVPN Server, OpenVPN Client
FTP Server	- FTP over SSL/TLS (explicit) - Max. Concurrent connections: 256 - Passive FTP Port Range Control - FTP Bandwidth & Connection Control - Unicode Support
Disk Management	- Online RAID capacity expansion - Online RAID Level Migration - HDD S.M.A.R.T - SCRUB Task - SHORT Test - LONG Test - Offline Test - Conveyance Test - Bad block scan - RAID recovery
iSCSI	- iSCSI Target - Virtual Disk Drive
Server Virtualization	- Supports Virtual Machines
Jails	- Support OS level virtualization for tamper proofing and maintaining sanctity
Power Management	- Wake on LAN - Scheduled power on/off - Automatic power on after power recovery

Technical specifications are subject to changes without notice.

Revision – 2.1, December 28, 2024

Software Specifications

Administration	- CLI and GUI support - HTTPS based user interface - HTTP/HTTPS connections - Email alerts - SNMP Traps (v2 & v3) - Dynamic DNS (DDNS) - UPS Support with SNMP & USB - Resource Monitor - Network Recycle Bin for CIFS/SMB - Comprehensive Logs (Events & Connections) - Syslog Client - Backup & Restore system settings - Web Based Quick Configuration Wizard
Access Right Management	- User Accounts - Groups - Shares - User Quota - Supports Active Directory Authentication, LDAP
Web Server	- HTTP/HTTPS connections - Supports WebDAV - Importable SSL certificate

NMS - UI based Configuration Utility Specifications

Product Overview

The equipment includes an NMS with an intuitive interface for secure, real-time monitoring of multiple Data Storage/NAS servers.The offered equipment provides a 24x7 live view of all operational parameters.

The NMS software includes a perpetual NMS license with no recurring fees, valid for the lifetime of the supplied NAS equipment.

The NMS is scalable, allowing the network administrator to add NAS servers anytime, both on-site and off-site, for disaster recovery and risk mitigation.

Hardware Specifications - NMS

Physical Machine	
Processor	Intel or equivalent
Number of Cores	16
RAM	64 GB
Storage	Minimum 1 TB NVMe
Additional Storage	Minimum 1 TB SSD
Display	1 x 21-Inch (or greater) Display for configuration 4 x 40-Inch (or greater) NMS Displays

Software Specifications - NMS

Operating System	Ubuntu 20.04 or higher
Web Server	HTTP, HTTPS
Licences	Software and license are included with the equipment at no additional cost or charge.

There will be no recurring or additional bi-annual / or annual recurring licence payments that are required to be made after the purchase of the equipment. The included licence is for perpetual use during the lifetime of the NAS data storage server equipment that is being offered.

Headquarters: Phoenix, Arizona

Orion Telecom Networks Inc.
20100, N 51st Ave,
Suite B240, Glendale AZ 85308
Phone: +1 480-816-8672,
Fax: +1 480-816-0115
E-mail: sales@oriontelecom.com

Regional Office: Miami, Florida

Orion Telecom Networks Inc.
4000 Ponce de Leon Blvd.
Suite 470, Coral Gables, FL 33146
Phone: + 1-305-777-0419,
Fax: + 1 786-536-4181
E-mail: sales@oriontelecom.com