InfoScale™ Security Deployment Guide

Executive Summary

InfoScale is widely deployed to provide high availability, storage management, and data protection for mission-critical enterprise workloads. Because InfoScale operates at the intersection of operating systems, storage, and clustering, it represents a high-value target for both external attackers and insider threats. A secure deployment is therefore essential not only for data protection, but also for service continuity and regulatory compliance.

This document presents a security deployment guide for InfoScale. It describes the security architecture, threat considerations, encryption mechanisms, and operational best practices required to deploy InfoScale securely in modern enterprise environments.

Introduction

High availability platforms are foundational to enterprise IT operations. InfoScale ensures application uptime and data integrity across clustered systems, but its privileged position within the infrastructure stack also demands rigorous security controls. Security weaknesses at the cluster or storage layer can undermine application-level protections and expose critical business data.

This document focuses on secure deployment practices for InfoScale on-premises, emphasizing encryption, trust establishment, access control, and operational security throughout the platform lifecycle.

InfoScale Security Architecture Overview

InfoScale security is implemented across multiple layers:

- **Host Layer:** Operating system hardening, kernel integrity, and privileged access controls
- **Cluster Layer:** Authentication, node trust, heartbeat communication, and fencing
- **Storage Layer:** Volume management, encryption, and access restrictions
- **Network Layer:** Segmentation, transport encryption, and firewall controls
- **Operational Layer:** Monitoring, logging, auditing, and incident response

Together, these layers provide defense in depth, ensuring that no single control failure compromises the overall system.

Threat Landscape and Risk Considerations

InfoScale environments face a distinct set of threats due to their role in managing shared storage and cluster coordination:

- Unauthorized access to physical or virtual disks
- Interception or manipulation of cluster communications
- Impersonation of cluster nodes
- Split-brain conditions leading to data corruption
- Abuse of privileged administrative access

A secure InfoScale deployment must address each of these risks explicitly through preventive and detective controls.

Secure Platform Foundations

Security begins with the underlying operating system. InfoScale should be deployed only on InfoScale-certified and supported distributions of the platform, with consistent OS and patched versions across all cluster nodes. Systems should be hardened using recognized benchmarks such as CIS (Center for Internet Security), unnecessary services disabled, and patch management rigorously enforced.

UEFI Secure Boot is strongly recommended to ensure kernel and module integrity. InfoScale kernel modules are digitally signed, enabling verification that only trusted code executes at the kernel level.

Use **Network Time Protocol (NTP)** time to synchronize time across all cluster nodes. NTP ensures **c**luster stability, accurate logging, and secure communications. Without time synchronization, InfoScale clusters risk false failovers, log inconsistencies, authentication failures, and certificate validation errors, all of which can compromise both availability and security.

For regulated environments, enable Federal Information Processing Standards (FIPS) mode during the initial installation to ensure all cryptographic operations utilize validated modules. Currently InfoScale supports **FIPS 140-2** compliance.

Encryption Strategy

InfoScale provides strategies for data at rest and in transit encryption. It is recommended that for secure InfoScale deployment that these strategies be employed as described in this section.

Data at Rest

InfoScale protects data at rest utilizing volume-level encryption provided by Volume Manager utilizing AES-256 standard. This ensures that data stored on disk remains confidential even if storage devices are lost, stolen, or accessed outside the trusted environment. Encryption is transparent to applications and can be applied consistently across all production data volumes.

Volume & Disk Group Encryption

InfoScale supports encryption at the volume level and disk group (set of volumes) level encryption and provides the following:

- **Key Encryption Key (KEK):** Securely wraps the Data Encryption Keys (DEK).
- **Online Re-keying:** Administrators can rotate keys without application downtime.
- **Deployment Tip:** Always upgrade to **Disk Group Version 300** or later to support the latest FIPS-compliant wrapping standards.

External KMS Integration

For scalable deployments, InfoScale integrates with external **Key Management Services (KMS)** via the **Key Management Interoperability Protocol (KMIP)** protocol (e.g., AWS KMS, HashiCorp Vault).

- **Workflow:**
    - Configure the KMS server hostname and port (Base64 encoded).
    - Deploy the **KMIP Secret** to the cluster nodes.
    - Establish a trusted communication channel using SSL (Secure Socket Layer) certificates (Custom CA or Self-signed).

Data in Transit

Administrative interfaces must be protected against interception and tampering. InfoScale supports encrypted communications using TLS (Transport Layer Security), ensuring confidentiality and integrity for management endpoints.

Network Security

Reliable and secure networking is essential for cluster stability. InfoScale deployments should use dedicated private networks for heartbeat and cluster communication, with redundant paths to prevent single points of failure.

Firewalls should restrict access to cluster ports and management interfaces. Configuring a firewall for InfoScale requires opening specific ports depending on which components (IOM, Cluster Server, or Replicator) you are using. The following tables list the standard ports required

for a typical InfoScale deployment on each component. Although User Datagram Protocol (UDP) is supported for some ports, it is recommended to use Transmission Control Protocol (TCP) as a best practice if available.

InfoScale Operations Manager (IOM)

These ports facilitate communication between the Central Management Server (CMS), managed hosts, and your web browser.

Port	Protocol	Direction	Description
5634	TCP	Bi-directional	**Primary Management Port:** Used for heartbeats and data uploads from managed hosts to the Management Server.
14161	TCP	Inbound	**Web Console:** Required for accessing the IOM web interface via a browser.
5636	TCP	Inbound	**Database Port:** Used by the Management Server to communicate with its internal database.
162	UDP	Inbound	**SNMP (Simple Network Management Protocol) Traps:** Required to receive real-time state change notifications (e.g., from VMware vCenter).

Cluster Server (VCS / Availability)

While most cluster communication (Low Latency Transport/Group Membership and Atomic Broadcast) happens over a private, non-routed heartbeat link, certain services require standard networking.

Port	Protocol	Direction	Description
14141	TCP	Bi-directional	**VCS Engine (High Availability Daemon - HAD):** Used for communication between cluster nodes and the VCS engine.
14144	TCP/UDP	Bi-directional	**VCS Notification**: listening port for the Notifier component
14149	TCP	Bi-directional	**VCS Authentication:** responsible for handling authentication requests within the VCS cluster
14150	TCP	Bi-directional	**Command Server (CmdServer):** essential for communication between cluster nodes, particularly for handling command requests in high-availability configurations.
14155	TCP/UDP	Bi-directional	**WAC Process:** The Wide-Area Connector (WAC) port for multi-site replication and failover.
14156	TCP/UDP	Bi-directional	**VCS Steward for Global Cluster Option (GCO):** enables the steward process to assist in decision-making for failover in a GCO environment, acting as a tie-breaker to prevent split-brain scenarios.

Volume Replicator (VVR)

If you are replicating data between sites for Disaster Recovery, these ports must be open between the Primary and Secondary nodes.

Port	Protocol	Direction	Description
4145	TCP/UDP	Bi-directional	**VVR Heartbeat:** Used for health checks between replication partners.
8199	TCP	Bi-directional	**Configuration Daemon:** Communication between vradmind daemons.
8989	TCP	Bi-directional	**Replication Sync:** Used by vxrsyncd for initial data synchronization.
49152-65535	TCP	Outbound	**Data Transfer:** Dynamic range used for the actual replication data stream.

General Infrastructure Ports

- **SSH (22):** Required for remote installation and command-line management.
- **Windows Management Instrumentation (WMI) (135):** Required for managing Windows-based hosts.
- **HTTPS (443):** Often used for connecting to cloud-based storage targets (AWS S3, Azure Blob) or for certain IOM add-ons.

Important Note: For **Low Latency Transport (LLT)**, which is the "heartbeat" of the cluster, it is highly recommended to use a **private, dedicated network**. If you must run LLT over a firewall and use UDP protocol, you will need to allow a minimum of 8 **UDP ports in the range of 49152 through 65535**.

Split-Brain Protection

To prevent split-brain conditions, InfoScale employs I/O fencing and quorum mechanisms. These controls ensure that only one set of nodes can access shared storage at any time,

preserving data integrity even during network partitions or node failures. Nodes that lose quorum or cluster membership are forcibly fenced off, preserving data integrity and preventing concurrent writes.

As a best practice, maintain redundant heartbeat networks and monitor the GAB (Group Membership and Atomic Broadcast) and LLT (Low Latency Transport) health using “gabconfig” and “lltstat” commands respectively. Although InfoScale supports a single coordination point server a minimum of three coordination points is recommended to enhance resiliency.

Secure Cluster

Configuring cluster services (VCS) in secure mode ensures that all the communication between the systems are encrypted and users are verified against security credentials.

With Secure Cluster, access control is done with a certificate-based framework and Lightweight Directory Access Protocol (LDAP)/Active Directory (AD) integration, ensuring only authenticated system users could access VCS components.

Role Based Access Control and Administrative Security

InfoScale leverages Role-Based Access Control (RBAC) to enforce the Principle of Least Privilege (PoLP), ensuring users have only the permissions necessary for their specific functions. By mapping identities to defined Privilege Levels—Administrator, Operator, or Guest—InfoScale separates duties among different users. This granular control can be applied globally at the Cluster level or restricted to specific Service Groups, allowing a designated user to manage high-availability (HA) for a particular application without impacting or even viewing the resources of other independent workloads.

To strengthen security and minimize high-risk direct root access, InfoScale integrates with AD or LDAP for centralized identity management. When configured in Secure Mode, InfoScale uses the hauser command or InfoScale Operations Manager (IOM) to bind OS-level users to these predefined internal roles. This integration creates a unified authorization framework.

Monitoring and Auditing

Continuous monitoring is critical for maintaining a secure InfoScale environment. Cluster membership changes, fencing events, authentication failures, and configuration changes should be actively monitored and alerted upon. **InfoScale Operation Manager (IOM)** is a centralized, web-based management console that can be used for this monitoring. It provides a "single pane of glass" for monitoring and controlling your entire InfoScale infrastructure across physical, virtual, and cloud environments. It simplifies complex administrative tasks—such as storage provisioning, cluster configuration, and fault monitoring—while offering comprehensive reporting and automated risk analysis to ensure application availability. InfoScale Operations Manager is

able to keep track of faults and events in the node, platform and application by utilizing InfoScale **Intelligent Monitoring Framework (IMF)**.

Here is a list of IOM security best practices to adhere to:

- Configure Single Sign-On (SSO) or LDAP/AD authentication for logging into the IOM Management Console. Once SSO is enabled, disable OS user authentication.
- Use role-based access control (RBAC) to manage who can perform operations, make changes, and monitor InfoScale servers. Available roles include Admin, Operator, and Guest. Assign permissions based on each user's required scope (perspective-wise).
- Enable the "Ask reason for all operations" setting to ensure users provide a reason for every change or operation.
- Use audit reports to track what changes were made, who made them, and the associated reason.
- When adding InfoScale servers to IOM for discovery and management, use the "Auto Configure" method. Download the gendeploy script when prompted, securely copy it to the target InfoScale server, run it to add the host, and delete the script after the host is successfully onboarded.
- Regularly update the IOM Management Server and IOM Agents with the latest patches and updates.

All administrative actions must be logged and audited. InfoScale offers support for audit log forwarding to local or remote servers for centralized management and IOM provides viewing and exporting of logs.

Ransomware Defense and Immutable Storage

A secure deployment includes mechanisms to recover from an active attack. InfoScale has such a mechanism called **SecureFS**. InfoScale's SecureFS is essentially a proactive data protection and recovery mechanism combining scheduled immutable snapshots, checkpointing, and application-aware consistency to defend against data corruption and ransomware attacks. SecureFS lets you recover data from these immutable checkpoints — either at file level or full volume level — helping rapidly restore operations after data corruption or malicious incidents.

Also, InfoScale introduced in release 9.0, **AI powered anomaly detection** of the InfoScale file system (VxFS). It acts as an early warning system designed to protect mission-critical applications and data from cyber threats—specifically ransomware and data breaches—by identifying "strange" behavior within the file system in real time.

For Secure Containerized Deployments

For vanilla Kubernetes deployments, InfoScale requires manual configuration to align with security best practices. This includes configuring a secure container registry, enabling image

vulnerability scanning, managing image pull secrets, enforcing RBAC policies, and ensuring encryption at rest as supported by the underlying storage and Kubernetes distribution.

In contrast, when deploying InfoScale on Red Hat OpenShift, many security capabilities such as secure and trusted image registries, integrated Common Vulnerabilities and Exposure (CVE) scanning, image signing and verification, RBAC enforcement, pull secret management, and encryption at rest—are natively provided by the OpenShift platform. InfoScale is designed to integrate with and leverage these OpenShift security features, reducing manual effort and helping organizations meet enterprise security requirements more consistently.

For transport-layer security, InfoScale in containerized environments supports both external Certificate Authorities (CA) and self-signed certificates, with automatic certificate rotation enabled through cert-manager integration. By default, TLS 1.2 is used and supports cipher suites TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256, TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

The table below outlines several recommended configuration settings for additional InfoScale security features for encryption and fencing for split-brain protection.

Security Control	Custom Resource Field	Recommended Setting
Disk Encryption	encrypted: true	Enable
SCSI-3 PR Fencing	enableScsi3pr: true	Enable
KMIP Key Management	infoscale-kmip-encrypt Secret	Configure
Dedicated Fencing LUNs	fencingDevice	Configure fencing

Conclusion

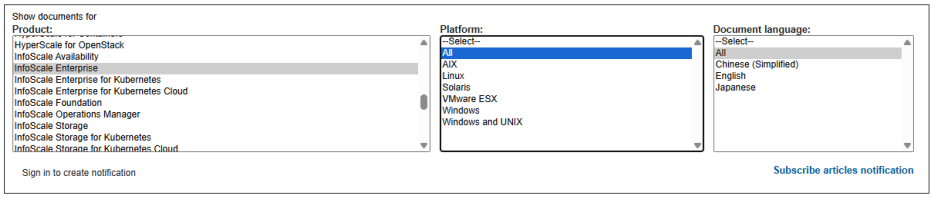
A secure InfoScale deployment is foundational to protecting enterprise availability and data integrity. By implementing layered security controls across hosts, networks, clusters, and storage, organizations can reduce risk while maintaining the resilience and performance InfoScale is designed to deliver. The practices outlined in this document provide a practical and compliant approach to deploying InfoScale securely in modern enterprise environments.

References

Please refer to the documentation depending on the platform you are deploying on.
The main InfoScale documentation page is at **https://sort.veritas.com/documents**. Once on this site, select InfoScale specific documentation or just InfoScale Enterprise, select platform

and then select language. Documentation for each version of InfoScale will be listed. Important documents that details the steps to configure the security practices described in this document are in:

- InfoScale Software Compatibility List
- InfoScale Hardware Compatibility List
- InfoScale Installation Guide
- InfoScale Administrator's Guide
- InfoScale Storage Foundation Configuration Guide
- InfoScale Operations Manager Installation and Configuration Guide
- InfoScale Operations Manager User's Guide



An empty cell indicates that no information is available.
"General" indicates that the applicable platforms or product versions are not defined.

InfoScale Enterprise

Product version	AIX	Linux	Solaris	VMware ESX	Windows	Windows and UNIX
9.1	Documentation	Documentation	Documentation	Documentation	Documentation	
9.0	Documentation	Documentation	Documentation	Documentation	Documentation	Documentation
8.0.2	Documentation	Documentation	Documentation	Documentation	Documentation	Documentation
8.0.1					Documentation	
8.0	Documentation	Documentation	Documentation	Documentation	Documentation	Documentation
7.4.3	Documentation	Documentation	Documentation			
7.4.2	Documentation	Documentation	Documentation		Documentation	
7.4.1	Documentation	Documentation	Documentation	Documentation	Documentation	Documentation
7.4	Documentation	Documentation	Documentation		Documentation	
7.3.1	Documentation	Documentation	Documentation	Documentation	Documentation	
7.3	Documentation	Documentation	Documentation		Documentation	
7.2	Documentation	Documentation	Documentation	Documentation	Documentation	
7.1	Documentation	Documentation	Documentation	Documentation	Documentation	
7.0.1	Documentation	Documentation	Documentation	Documentation	Documentation	
7.0	Documentation	Documentation	Documentation	Documentation	Documentation	