VANTAGEO-Server

Suite Hardware Management Platform

Product Description

VANTAGEO PRIVATE LIMITED

LEGAL INFORMATION

Statement on the Use of Third-Party Embedded Software:

If third-party embedded software such as Oracle, Sybase/SAP, Veritas, Microsoft, VMware, and Redhat is delivered together with this product of VANTAGEO, the embedded software must be used as only a component of this product. If this product is discarded, the licenses for the embedded software must be void either and must not betransferred. VANTAGEO will provide technical support for the embedded software of this product.

About This Manual

Purpose

This manual describes the VANTAGEO-VSS (hereinafter referred to as the VSS) in details, including product positioning and characteristics, product architecture, functions, security,reliability design, network architectures, interfaces, technical specifications, and compliant standards and protocols, so that users can fully learn about the VSS.

Product Overview

1.1 Product Introduction

The VSS is unified O&M management software for VANTAGEO servers and storage devices usedin IT scenarios. It implements unified management of VANTAGEO servers and storage devices in GUImode. The VSS provides VANTAGEO servers with enhanced full-lifecycle management capabilities such as resource management, batch configuration, firmware and driver upgrade, fault diagnosis, OSdeployment, power consumption management, report management, and remote fault reporting, which effectively improve O&M efficiency and reduce O&M costs. In addition, the VSS provides a variety of northbound interfaces for interconnection with OSS.

1.2 Product Characteristics

The VSS has the following characteristics:

- Supports centralized management of multiple devices, including a full series of VANTAGEO serversand storage devices.

- Supports flexible deployment of physical machines and VMs in multiple scenarios, IPv4/IPv6dual-stack network architecture, and management of a maximum of 3000 devices.
- Provides the centralized resource management function to help users manage servers andstorage devices in an all-round manger.
- Provides the centralized alarm management function to allow O&M personnel to locate and troubleshoot faults so as to avoid service interruption.
- Provides the centralized performance management function to manage the KPIs of serversand learn about performance bottlenecks.
- Configures servers in batches through a profile so as to achieve stateless configuration ofservers.

- Manages the life cycle of the firmware of each server through firmware check, upgrade, and validation, thus improving the firmware management efficiency.
- Provides northbound interfaces such as the RESTful, SNMP, Syslog and SFTP interfaces tointegrate with the OSS system.
- Supports server fault diagnosis and out-of-band preventive maintenance, helping O&M personnel monitor the health status of server components.
- Supports automatic deployment of out-of-band OSs in batches.
- Supports power consumption management by monitoring the total power consumption of devices in equipment rooms or cabinets and the cabinet space usage in a unified manner.
- Supports maintenance management which allows you to implement management of device maintenance information in GUI mode.
- Supports multi-dimensional report management that allows you to customize reports onserver alarms, performance, and assets.
- Supports remote fault reporting and automatic service ticket creation and submission, thus achieving intelligent O&M.

Product Architecture

Table 2-1 VSS Module Function Descriptions

Module	Description
Alarm management	Obtains and analyzes hardware alarms through SNMP Trap or Redfish subscription.
Performance management	Periodically collects performance data of devices, such as CPU usage, power, temperature, GPU temperature, and GPU power.
Module	Description
Resource management	Supports device addition, deletion, automatic discovery, and periodic collection of asset information of devices.
Log management	Collects logs reported by devices and manages the operation logs, login logs, and system logs of the VSS.
User management	Manages the authentication and authentication management modules of local users and external AD users.
Security management	Manages accounts, passwords, session policies, access control, and other security information of the VSS.
Firmware management	Upgrades the firmware (such as the BMC, BIOS, and standard card) and driver of VANTAGEO servers.
Configuration management	Configures the BMC, BIOS or RAID on a VANTAGEO server, checks the configuration, and supports importing and exporting the profile. Pre Configured Profiles with Valid Config information are kept in the repository. The VSS supports the abstraction of the BMC, BIOS, and RAID configuration information of a server into a profile. Through the import and export functions, the profile can be copied quickly to deploy Automatically deploy the desired profile on the desired servers using batch task Thus it delivers hardware configurations to other servers in batches, & improving the efficiency of device onboarding.
OS deployment	Deploys commercial OSs in batches on VANTAGEO servers. Create Configuration Profile or Profiles Templates with required configuration and the ISO image of the desired Operating system and store in the repository. Automatically deploy the OS and Configuration on the desired servers using a batch task
Fault diagnosis	Supports hardware diagnosis of VANTAGEO servers and outputs diagnosis reports.

Power consumption management	Periodically collects server power and displays it by level, and detects the power consumption of each cabinet.
Technical service	Supports maintenance management and remote fault reporting. ● Maintenance management: supports the import of the maintenance data of VANTAGEO servers, and displays the warranty periods of the servers. ● Remote fault reporting: supports automatic fault reporting and service ticket creation.
Report management	Supports report customization based on assets, alarms, and performance data, and flexible data analysis.

The VSS provides reliable management of the entire devices, alarms, resources, performance, logs, configurations, firmware, users, and security of VANTAGEO servers and storagedevices.

Device Management

Management Mode

Devices can be added as the managed devices of the VSS in the following ways:

- Manual addition: Add a device manually.
- Batch import: Import all devices at a time through a template file.
- Automatic discovery: Add devices through automatic scanning in accordance with the IPnetwork segments.

VANTAGEO rack servers and disk arrays that can be managed by the VSS are as follows:

Supported Operations

- Servers: 2230-RE ,1230-RE,2240-RE,1240-RE

The VSS supports the following operations on a server:

- Power on, power off, and restart the server.
- Download BMC logs.
- Enable HTML5 KVM.
- Modify and manage the BMC usernames and passwords.
- Lit the UID indicator.

Note

Operations on a server are strongly related to the BMC version. You need to determine whether thecurrent BMC version supports related operations.

Alarm Management

The VSS supports real-time monitoring of device alarms. VSS has a feature of Auto Log Collection from the connected from the connected Servers. In this case, O&M personnel can handle hardware faults in a timely manner. Alarm management contains the following functions:

- Alarm display

  Logs are analyzed by VSS . It uses the learnings from the systems and the VSS's intelligent analytical engine to give out Alerts /Alarms. The Alerts / Alarms will be both Predictive and Immediate in nature

  Obtains device alarms through SNMP Trap or Redfish subscription. You can browse alarmsin the active alarm list, and view the cleared alarms in the historical alarms.

- Alarm acknowledgment

  Provides a method for determining whether an alarm is handled. Alarms that are already handled and alarms that are not handled can be distinguished in accordance with the alarmacknowledgment status.

- Alarm clearing

  Supports alarms manually clearing. Cleared alarms are transferred to the historical alarmdatabase and no longer displayed in the active alarm list.

- Alarm export

  Supports condition-meeting alarms exporting into a CSV file.

- Alarm masking

  → Supports alarm masking based on conditions such as time, period, alarm source (alarmgeneration device), alarm code, and alarm level. Alarms that meet the conditions are suppressed and not displayed in the alarm information.

  → Alarms of a specified server can be masked in a specified period of time for servermaintenance.

- Alarm synchronization

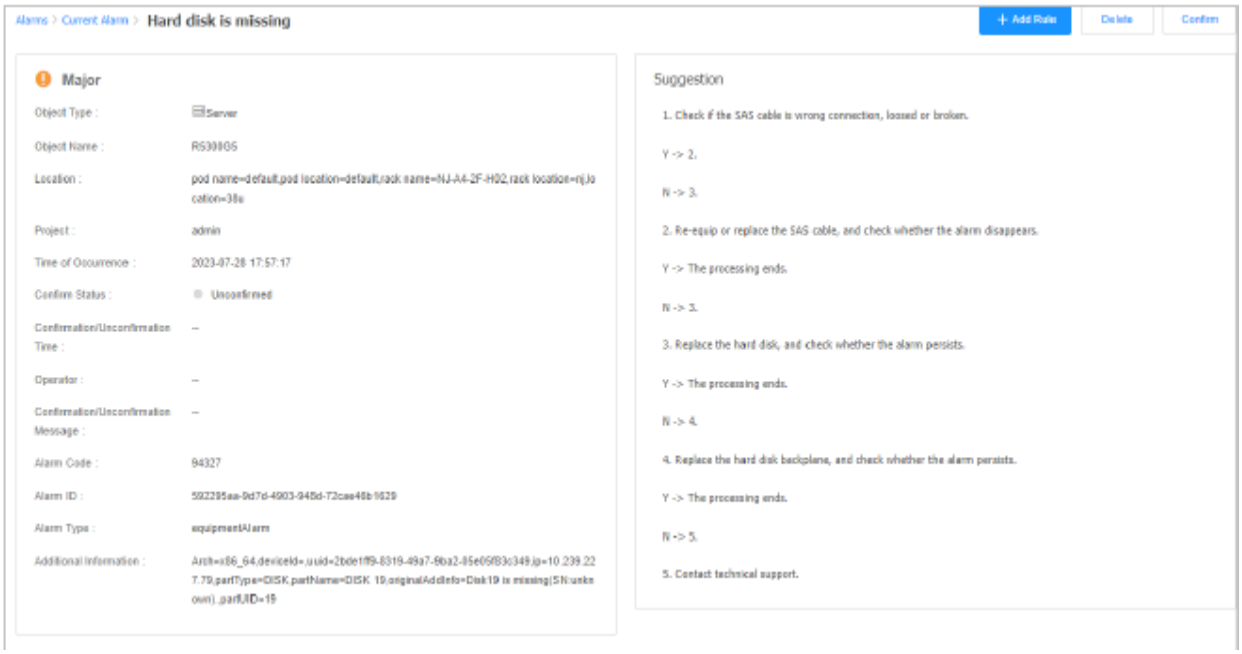
  Supports the application of alarm loss detection and automatic synchronization functions to VANTAGEO servers to ensure that alarms on the system side and the device side are the same.

- Remote notification

  Sends emails to notify O&M personnel of alarms in real time in accordance with the rules formulated by users.

  VSS based on the type of Alert gives out actionable remediation using the system learnings and intelligent analytical engine.

Viewing Alarm Details – Suggestions from Proactive Analytical Engine



Resource Management

The VSS shows the location of the devices in a data center through the rack view, and the detailed information of a device and its components through the detail view. In this way,resources can be managed in an all-round manner. Resource management contains the following functions:

- Displaying device information
  - → Device information: device model, manufacturer, serial number, asset label, firmwareversion number, power mode, and maximum power.
  - → Processor information: name, manufacturer, model, CPU clock speed, number of cores,and hyper-threading status.
  - → Memory information: slot, type, model, manufacturer, capacity, and frequency.
  - → Controller information: slot, model, and firmware version.
  - → NIC information: slot, model, interface type, number of ports, serial number,manufacturer, and firmware version.
  - → Network interface information: name, interface type, MAC address, rate, and port status.
  - → FC interface information: name, interface type, WWN, and rate.
  - → Logical disk information: name, RAID level, and capacity.
  - → Hard disk information: name, serial number, slot, model, capacity, interface type, mediatype, manufacturer, firmware version, remaining SSD lifespan, and disk partition usage.
  - → Power supply information: slot, name, type, and rated power.
  - → Fan information: slot, maximum fan speed, actual fan speed, minimum fan speed, andfan speed ratio.
  - → Temperature sensor information: air inlet and CPU.
  - → GPU information: vendor, model, display memory, and bandwidth.

- Exporting asset details

  Exports the details of all assets in batches.
- Operating devices

  Supports remote control over a single device, including power-on, power-off, and restart.

Performance Management

The VSS manages the performance of the servers. It collects, analyzes, and graphically displays real-time and historical out-of-band performance data to help O&M personnel analyzeand predict the resource bottlenecks, effectively evaluate resource usage, and optimize deviceperformance.

---

devices through the dedicated management network.

The functions of performance management are as follows:

- Automatically collects all the performance indicators of a server, including the CPU usage,memory usage, power, air inlet temperature, GPU temperature, fan speed, current, and voltage.
- Supports customization of collection periods and flexible management through tasks. After the indicators of a server are collected, the historical performance data of the server can beviewed.
- Displays real-time and historical performance trends in visualized curves or tables.
- Displays the top N performance data of the data center on the **OverView** page of theVSS portal.

Log Management

The VSS supports log management, providing effective help in routine O&M and problemlocation. The available log information and supported management functions include:

- Operation log
  - → Records the operations initiated by operators that cause changes in the system, and the operators' names, operation time and operation contents. Operation logs cannot bemodified.
  - → Supports log query to facilitate backtracking.
- Security log

  Records security-related actions, such as user login and logout.
- System log

  Records key information automatically generated by the system during operation or task execution for backtracking.
- Hardware log

  Collects hardware logs reported by devices through the Syslog interface, such as theoperation logs, system logs and login logs of a BMC on a server.

Configuration Management

The VSS supports the abstraction of the BMC, BIOS, and RAID configuration informationof a server into a profile. Through the import and export functions, the profile can be copied quickly to deliver

hardware configurations to other servers in batches, thus improving the efficiency of device onboarding.

- Profile: Sets parameters for the BMC, BIOS, and RAID of a VANTAGEO server.
  → A template can be exported from a benchmark server (a server whose configurations provide a benchmark for the configurations of other servers) and edited online to form aprofile, based on which the configuration information of other servers can be checked inbatches.
  → For a server with different configurations, you can quickly copy the configurations in theprofile to this server by binding the profile to the server.
- BMC configuration of a server: Configures items such as NTP, time zone, AD, heat dissipation mode, Syslog, SNMP and service port.
- BIOS configuration of a server: Configures items related to boot options, PXE, virtualization,power, processor, memory and console.
- RAID configuration of a server: Supports the configurations of VANTAGEO-developed RAID controller cards, PMC RAID controller cards and AVAGO RAID controller cards.
- Server configuration check: Checks the BMC and BIOS configurations of servers in batches.The check results can be exported to an Excel file.

Firmware and Driver Management

The VSS supports the management of the following firmware and drivers:

VSS auto discovery capability allows to manage the Vantageo devices once connected on the accessible network without any manual intervention

- Firmware version
  The BMC, BIOS, and part versions of VANTAGEO servers can be managed.

  Note

  Parts include the NIC, RAID controller card, and HBA card.

- Driver type
  → NIC: Intel X710 and Intel EXL710.
  → FC HBA: QLE2742.
  → RAID: VANTAGEO RS241_V2-16i.

Firmware and driver management of the VSS has the following features:

- Firmware/driver package repository
  Uploaded firmware/driver packages are stored in the repository for firmware/driver upgrade
  VSS will use learnings from systems and with the help of intelligent analytical engine search the updated Firmwares on the Vantageo Internet repository..

- Baseline version
  A baseline version can be created to manage different types of firmware and drivers ofservers in a unified manner for one-click upgrade. VSS keeps a data of all the Firmware version

installed on the managed devices

- Validation policy

  VSS without any manual intervention will automatically download the Firmware into the local repository and send an alert about the availability of the new Firmware.

  Upgrade and validation are separated. Immediate validation and manual validation are supported, thus improving the upgrade security.

  .

- Firmware check

  → A firmware consistency check task can be created and associated with a specifiedfirmware baseline to check the firmware of a group of servers or a specified server.

  → The firmware consistency check task can be executed immediately or at the specifiedtime based on the setting of an execution policy.

  → You can view the check report in the check result area or on the firmware check menu.The firmware of the device that is not the same as the firmware baseline is displayed.

  Deployment/execution

  Firmware are automatically updated on the respective Servers based on the scheduled task defined by the Administrator. Firmware update needs a reboot to have the new firmware in effect.

Parameter	Description
BIOS Version validation policy	Select the BIOS version validation policy.
	> Effective Immediately: The devices are automatically restarted to apply the new version. But in this way, services may be interrupted
	> Effective Manually: You need to manually apply the new versionon the Version Status page.
BMC Version validation policy	Select the BMC version validation policy.
	Default: Only the standby BMC firmware is upgraded.
	MainStandby: Both the active and standby BMC firmware are Upgraded
Plan Strategy	Select the upgrade task execution policy.
	> **Execute Immediately**: The task is executed immediately.
	> **Schedule Execution**: You can click to set the task execution time.

User Management

The user management functions of the VSS include the following:

- Local user management

  → Local users can be viewed, added and deleted, and their passwords can be modified.

→ Local users can be granted time-based permissions.

- External user management

  → Supports interconnection with the OpenLDAP or the Active Directory servers, and loginto the VSS through the user domain in the domain controller, and external users in the group domain and their passwords to ensure system security.

  → Supports the LDAPS protocol, and multiple login attributes such as mail, common name(CN), surname (SN), and sAMAccountName.

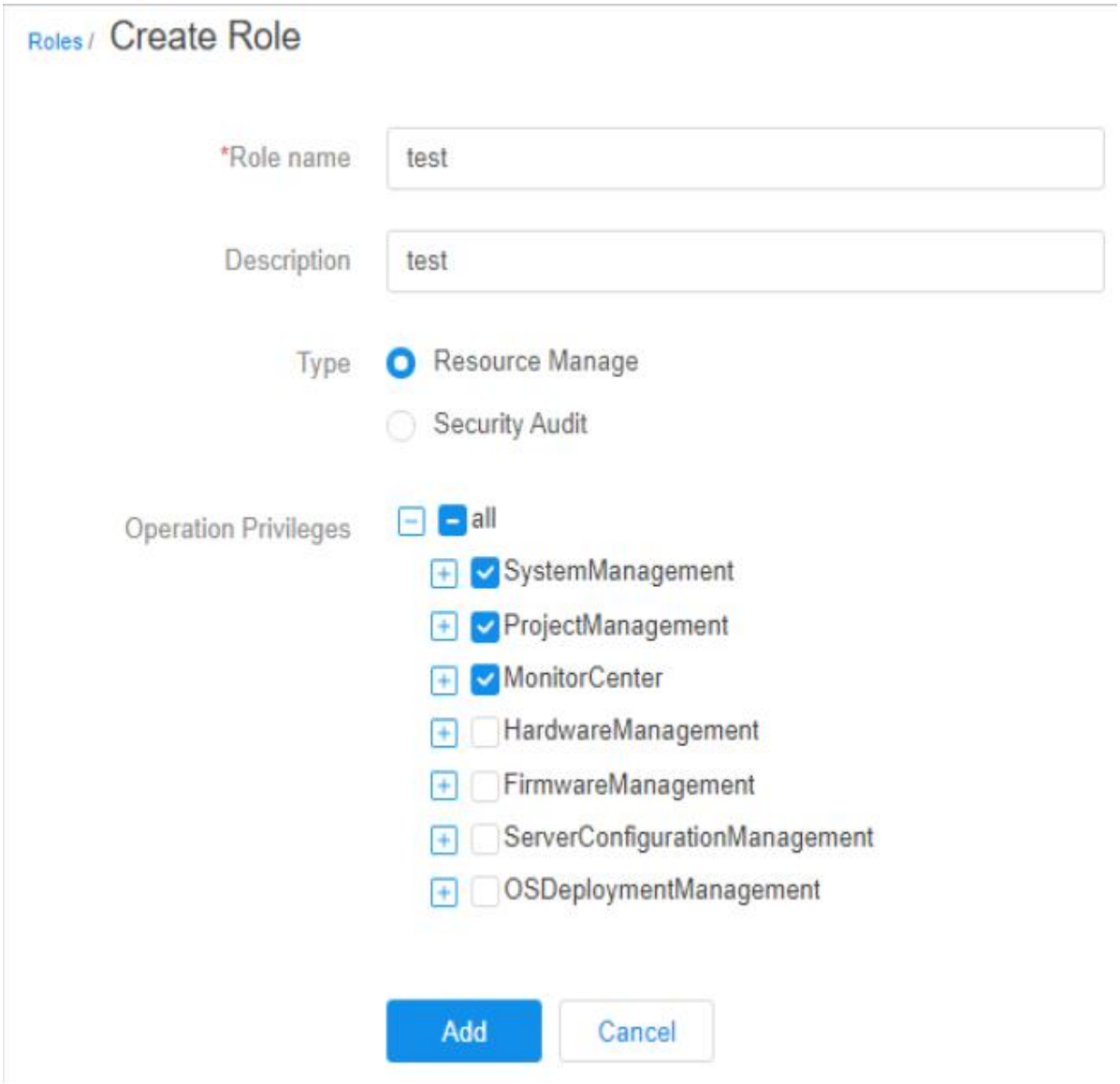
VSS Support USER Management for Local user and External User.

The default roles such as admin and Operator already exist on the VSS portal. If the default roles do not match the functional attributes of the internal user to be created, you need to create the role.

Various Operational Privileges are available such as

- System management ,
- Project management ,
- Monitor center .,
- Hardware Management ,
- Firmware Management,
- Server config management,
- OS deployment management

To choose basis on the soles the user View gets customized.



Security Management

Through proper security parameter settings, the VSS can effectively prevent unauthorized users from intruding into the system and ensure system data security.

User permissions

Login authentication

Access control

Certificate management

Session management

Account security

Secondary authorization for high-risk operation

Security Management

Through proper security parameter settings, the VSS can effectively prevent unauthorizedusers from intruding into the system and ensure system data security. Security management contains the following functions:

- User permissions
  - → Supports RBAC.
  - → Provides permission control.
  - → Supports customized roles.
  - → Provides access time control.
- Login authentication
  - → Supports authentication based on SMS verification codes and graphic verification codes.
  - → Supports SSO and OAuth 2.0.
- Access control
  - → Provides the time control mechanism for user login.
  - → Supports password blacklist.
  - → Supports IP address blacklist and whitelist.
- Certificate management

  Supports both the CA certificate and self-signed certificate, and uses HTTPS for all browser operations and RESTAPI calling.
- Session management
  - → Logs out once the session expires.
  - → Protects the security of the session IDs.
  - → Supports configuring the number of on-line sessions.
- Account security

  Allows you to sets security policies, such as password complexity, validity period, reuse, andlocking.
- Secondary authorization for high-risk operations
  - → Sets whether secondary authorization is needed for high-risk operations, such as serverpower-off and restart.
  - → By default, the `admin` user has the permission to perform secondary authorization forhigh-risk operations. Other users can obtain this permission only when the secondaryauthorization policy is enabled.
  - → If a common user performs a high-risk operation, the operation takes effect only when auser with the secondary authorization permission approves this operation.
- License
  - → Supports license import.
  - → Supports querying the validity period and function of a license.

Fault Diagnosis

The VSS supports out-of-band hardware preventive maintenance of servers, and identifiespotential faults in advance based on BMC log analysis. The following functions are supported:

- Checking the health status of servers and server components, including the entire devices,CPUs, memory, hard disks, RAID cards, NICs, PSUs, and fans.
- Supporting in-depth preventive maintenance of hard disks, remaining lifespan tracking ofSSDs, and SMART tests of SATA and SAS mechanical hard disks.
- Supporting automatic preventive maintenance at a specified time.
- Outputting preventive maintenance reports in HTML format, and classifying the preventive maintenance results by severity.

OS Deployment

To deploy OSs through the PXE, you need to access service networks. Therefore, you cannotdeploy OSs through the PXE when only out-of-band networks are available. The VSS supports automatic out-of-band OS deployment. The functions are as follows:

- Mounting OS images

  OS images can be uploaded manually.

  Deploying OSs

  Out-of-band networks and Redfish interfaces are used to mount OS images. Deployment parameters can be configured in GUI mode and OSs can be deployed in batches.

  .

Power Consumption Management

Due to the increasing power consumption of servers, the current power supply planning of a data center room may be difficult to meet the power consumption requirements of servers in thefuture. Even if the power consumption of each server in a cabinet is within the normal range, the total power consumption of the cabinet may exceed the planned capacity. To solve the

above problems, the VSS supports energy efficiency management at different levels. Thefollowing functions are provided:

- Periodically collecting the power of each server, and displaying the power at different levels including equipment room, cabinet, and device.
- Supporting the setting of the rated power of each cabinet. When the total power of thecabinet exceeds the rated power, the system notifies the user of the overload risk.
- Supporting the display of the space usage of each cabinet, through which you can adjust the deployment of servers in the cabinets to effectively use the space of each cabinet.

Maintenance Management

The VSS supports the management of equipment maintenance information in GUI mode.The following functions are provided:

- Maintenance statistics
  → Supporting the import and export of server maintenance information in batches.
  → Displaying the number of managed servers in a histogram, including the number of servers whose warranty period has expired and the number of servers whose warrantyperiod is about to expire.
- Maintenance list
  → Displaying the basic maintenance information about managed servers.
  → Providing the advanced search function. You can query servers by maintenance typeand remaining warranty period.

Remote Fault Reporting

The VSS supports the remote fault reporting function, which is displayed as Call Home onthe VSS portal. The VSS creates service tickets and automatically reports faults to theVANTAGEO technical support center through the Internet to achieve intelligent O&M,

Remote fault reporting provides the following functions and features:

- Networking requirements
  The VSS is installed on two network planes, and the northbound network is connected tothe Internet. If the northbound network cannot be directly connected to the Internet, a proxy server needs to be provided by the customer.
- Information security
  Service tickets are created and submitted based on device alarms, and logs are notcollected.
- Transmission security

HTTPS is used for encrypted transmission.

- Use security
  → Alarm codes to be reported can be selected based on the alarm level or as required.
  → Only registered users of the Web portal of the servers and storage products (https://www.vantageo.com) can successfully submit service tickets.
- Reliability design
  → Delayed submission of service tickets is supported to avoid reporting faults that arerecovered instantaneously.
  → The VANTAGEO technical support center sends heartbeat keep-alive messages to the VSS periodically. When the VSS is down or disconnected, the VANTAGEO technical support center sends a service ticket because it does not receive a response from the VSS within the specified time.
- Service ticket management
  The details and status of each service ticket are displayed. You can delete, refresh, orcancel service tickets as required.

Report Management

The VSS provides the data analysis and statistical chart display capabilities through report management. You can query indicators in multiple dimensions as required, and quickly focus on key data through flexible data filtering to implement self-service O&M analysis and regular reporting.

Report management provides the following functions and features:

- Covering various O&M scenarios
  Presets data sets and templates for typical service scenarios. The data sets include KPIs of servers and disk arrays, and the templates for the assets, performance, and historical alarms of servers and disk arrays are available. Together with the customization capability,the report management function can fully cover various O&M scenarios and meet user requirements.
- Supporting flexible report customization
  → Analyzes data in periodic reports by hour, day, week or month to obtain the trends ofdata, providing a powerful basis for decision-making.
  → Based on the server and disk array assets, performance, and historical alarm templates preset in the system, algorithms can be customized and new KPI data can be generatedto present the final report in a way that meets your requirements.
- Providing multiple data display modes
  → Data can be displayed in tables and graphs, and the "Roll Up" and "Drill Down" functionsare provided.
  → The inventory, performance, and historical alarm reports of servers and disk arrays canbe exported in Excel, CSV, and text formats for query and audit, meeting daily O&M requirements.

→ Asset data reports can be generated based on four dimensions, that is, equipment room, rack, device, and component, and the data can be displayed in details or in asummarized way based on the time and space dimensions.

→ Alarm data (including the total number of historical alarms and alarm level distributionstatistics) can be displayed in details or in a summarized way based on the time and space dimensions

→ Performance data reports can be generated based on three dimensions, that is, equipment, component, and indicator, and the data can be displayed in details or in asummarized way based on the time and space dimensions.

Supporting flexible data analysis Reports can be filtered by object or indicator for data analysis, which helps you concentrateon key data and learn about service trends

.

Interfaces

REST API for interaction data with automation, ticketing and other tool

As IT management software, the VSS system manages hardware resources such as server storage devices. The details are as follows:

- Security: The system provides account authentication and authorization through the Keystone component.
- Content: The system allows users to select and subscribe to desired content through indicator subscription interfaces.
- Management: The system provides extensive interfaces such as CM (Configuration Management), FM(Fault Management), PM (Performance Management), and log management interfaces for obtaining various types of O&M data.
    - Interface Information Description
    - The VSS system provides interfaces for interaction with the NBME (Northbound Managed Element). The purpose is to collect hardware resource performance KPIs, monitor status, and report resource changes and faults.

The interfaces are as follows:

- Resource query interface: involves hardware resource query.
- Resource change reporting interface: involves hardware resource change

notifications.

- Resource monitoring interface: involves hardware resource status monitoring.

- Resource performance management interface: involves the query of hardware resource performance KPIs.
  - Resource alarm management interface: involves reporting hardware resource alarms.

Southbound Interfaces

The VS`S/Uniview communicates with lower-level server devices and storage devices through southbound interfaces. Southbound interfaces include:

- Server device interface

  The VSS server can obtain control information and resource information about lower-level server devices through the SNMP and Redfish interfaces. For interface protocols supported by lower-level server devices, refer to Table 5-1.

  Note

  The Redfish interface must be used when enhanced features are used.
- Storage device interface

  The VSS obtains disk array management information, alarm information, and performance data through the SMI-S, SNMP and HTTPS interfaces.
- Log Interface

  The VSS obtains the logs of devices connected to the VSS through southboundinterfaces through the Syslog interface.

Northbound Interfaces

The VSS interconnects with the upper-level OSS through northbound interfaces to providealarm, performance, status, and resource data for the upper-level OSS. The northbound interfaces include:

- SNMP interface

  The VSS reports alarms through the SNMP interface. It supports SNMPv2c andSNMPv3.
- Syslog interface

  The VSS reports alarms through the Syslog interface.

- RESTful Interface

  The VSS queries resource, assets, and performance statistics information, andsubscribes to alarms through the RESTful interface.
- SFTP interface

  The VSS reports logs, performance, and other result files through the SFTP interface.

Security

Complying with the industry's strict security standards, the VSS provides effective protectionfor users' information security in terms of physical environments, networks, platforms, application interfaces, and data.

Physical Security

It is recommended that the VSS be installed on a VANTAGEO-developed 2U server. Taking theVT 2230-RE as an example, the following measures are taken to maintain physical security:

- Supports TPM and TCM, and provides all-round security measures such as unique identification, system login encryption, folder encryption and network communication encryption.
- Uses Redfish and SNMPv3 for the BMC:
  → Redfish provides the next-generation standard chassis management interface protocolwith a higher security level than IPMI 2.0.
  → SNMPv3 provides the SHA authentication algorithm and AES encryption algorithm.
- Supports hard disk security management, hard disk status management, and hot swapping.
- Supports chassis intrusion detection to report alarms for unauthorized operations.
- Applies an active/standby redundancy pattern to key components such as fans, powersupplies, BMC boots and BIOSs.

Network Security

You can maintain network security through the following ways:

- Dividing network security areas
  The network is divided into isolation areas, trusted service areas, and management areas. The areas are isolated from each other to improve the intrusion prevention capability of thenetwork.
- Separating network security responsibilities
  The VSS network is divided into the data synchronization network, northbound network, and out-of-band management network of hardware resources to ensure that services do notaffect management operations.
- Protecting against network attacks
  To detect and block attacks from the Internet and external networks, you are recommendedto deploy IDS and IPS at the external network boundary and security area boundary to prevent protocol attacks, violent attacks, port or vulnerability scanning, virus or Trojan attacks and other intrusion activities.

- Preventing Web attacks

  To protect Web application services and systems, a WAF is deployed on the network boundary to deal with Web attacks, such as DDOS attacks, SQL injections, XSS attacks andCSRF attacks.

Application Security

The VSS takes the following measures to maintain application security:

- Performs routine security hardening on the operating system to ensure that application programs are running in a secure environment.
- Securing accounts and passwords

  → Allows users to set password complexity, password validity period, and account lockoutthreshold.

  → Forbids passwords from being saved in plain text or in cipher text processed by insecurepassword algorithms.
- Controlling access

  → Enables the MAC policy due to the fact that different services in the OS are used bydifferent users or groups.

  → Supports role-based permission management in applications to minimize themanagement permissions and access scope.
- Maintaining API security

  → Authenticates the identity of API access.

  → Encrypts and transmits API data.
- Using TLS, HTTPS and SFTP instead of insecure protocols

Data Security

The VSS takes the following measures to maintain data security in terms of confidentiality,integrity, availability, durability and traceability:

- Carrying out identity authentication and control on data access.
- Encrypting data transmission procedures through HTTPS, TLS, and other security protocols.
- Using keys to encrypt and store sensitive data.

Reliability Design

The VSS provides highly reliable design for networking, architecture, and data to ensuresystem stability and security.

Network Reliability

The VSS guarantees the network reliability from the following aspects:

- Using Pacemaker+Corosync as HA software to avoid single point of failures
  The HA software supports dual-node cluster configuration, in which one node operates asthe active node, and the other as the standby node. The two nodes operate together to provide external services.
  The components of the VSS operate on the active node. If the active node is faulty(the network, file system, or applications are abnormal), the services provided by the components are stopped on the active node and restarted on the standby node.
- Supporting network interface detection and binding
  The OS can automatically detect the abnormality of a certain network interface and switchover the physical network interface, so as to ensure the high availability of the network.

Architecture Reliability

The VSS software uses the IAG architecture and guarantees the reliability of thearchitecture from the following aspects:

- Loose coupling design
  → Different service logic uses different microservices to provide capabilities.
  → APIs (RESTful interfaces) provide the external access capability for microservices andsupports the invocation of capabilities between microservices.

→ On the access point for external services, microservices can be added or deleted asrequired.

→ The IAG implements message routing to provide a unified service entrance.

- Fault tolerance capability
  → If a microservice is faulty, other microservices can operate properly.
  → In a large-scale scenario, when the processing capabilities of a microservice areinsufficient, multiple instances can be started to provide support.
- Fault monitoring and handling
  → During program running, the supervisor process is also started.
  → If a microservice aborts, the supervisor process restarts this service.
- Hot patches
  To apply a hot patch online, you only need to restart a microservice. The restart does notaffect other modules or services.

Data Reliability

To ensure data reliability, the VSS provides the following functions:

- Data storage
  → Saves database data on a local disk.
  → The local hard disk backs up data in RAID mode.
- Data backup
  → Backs up the data in the database periodically, and reserves some data copies.
  → Flexibly sets the scheduled backup time and sets the backup interval in accordance withthe volume and importance of the data.
  → Stores the backup data on external storage devices.
- Data recovery
  → Automatically restores the latest backup data when data is damaged.
  → In other cases, you need to manually restore the data.

Configuration Requirement

To ensure the proper operation of the VSS, the software and hardware of the VSS needto meet the following requirements. For details, refer to Table 8-1.

Table 8-1 VSS Configuration Requirements

Type	Requirement	Description
Deployment scenarios	● Bare machines or VMs are supported. ● VM types including VMware, KVM, and Hyper-V are supported.	It is recommended that you deploy the VSS on a VM. If you deploy the VSS on a physical machine, it is recommended that you use a VANTAGEO rackserver.
Resource requirements	● CPU: 8-core, 2 GHz ● Memory: 20 GB ● Hard disk: 350 GB	With this configuration, a maximum of 3000 devices can be managed.
Database	PostgreSQL is provided.	Third-party databases are not supported.

Supported Policies

VSS Manages Varius categories of Policy Management and the execution is actioned as per defined policy.

- Authentication Policy for user Management
- Diagnostic Policy
- Configuration Policy
- Speed regulation policy for Fans
- Power restore Policy
- BIOS parameter validation policy.
- BIOS Version validation policy
- user Creation Policy
- User Security Policy
- User Access Policy
- System Management Security Policy
- privacy Protection Policy
- secondary authorization policy
- SMS Verification Code Policy
- Authentication Policy
- password replication policy
- password unique policy
- User inactive policy

Compliant Standards and Protocols

Compliant Standards

- IPMI
- SMI-S
- Redfish: A new-generation standard for the management of servers and other hardware,using the RESTFul interface to express data and facilitate management

Compliant Protocols

- RFC 1157: SNMP V3
- SSH V2
- HTTPS: TLS 1.0 and its later versions
- SFTP
- LDAP
- SNMP