accelops

DATASHEET

AccelOps Integrated Security, Performance, and Availability Monitoring Application

Simplifying complex real-time, cross-domain analytics for more secure, responsive and adaptive IT infrastructures

Assure service availability and increase operational efficiency with integrated real-time data center monitoring, alerting, analysis, and reporting

The AccelOps monitoring application offers a seamlessly integrated platform for the collection, monitoring, analysis, alerting, and reporting of all IT event, log and performance data. A patented real-time analytics engine correlates events, logs, and performance metrics across the entire physical and virtual data center infrastructure including servers, storage, network, security devices, users, location, and applications in a single application. Built-in rules, which may be easily customized by the user if desired, alert IT to malicious activity or performance-impacting events. From a "single pane of glass," IT can monitor all data center activities and resources whether on-premise, remote, or in the cloud.

Automated Discovery and Configuration Monitoring Database (CMDB)

- Discover network devices, servers, storage, users, and applications in both physical and virtualized environments by combining SNMP, WMI, Telnet/SSH, LDAP, VMware VM-SDK, HTTP(S), Microsoft RPC, Cisco SDEE, JMX and JDBC
- Discover hardware and inventory information, bios, configuration, installed applications, running processes and services, interfaces, storage, open ports, and installed patches
- Map layered relationships such as virtual to physical machines, wireless access points to controllers, and network devices to log/management servers
- Automatically categorize discovered entities into groups using customizable knowledge base
  - Functional device groups – firewalls, router/switches, VPN gateways, storage, etc.
  - Infrastructure application groups – DNS servers, DHCP servers, AAA servers, etc.
  - User application groups – web servers, application servers, database servers, mail servers, etc.
- Dynamically create a configuration management database (CMDB) and automatically generate detailed layer 2 and layer 3 network topology maps
- Schedule periodic discovery to automatically detect new devices, network, server and directory service configuration changes, and maintain updated CMDB and network topology
- Fast adjacency-driven, smart discovery in addition to full IP range scan
- Create reports for inventory management, capacity planning and compliance

Multi-faceted Data Collection

- Multi-faceted collection of SNMP and WMI data, hardware status, system files, system logs, application logs, network device logs, directory service objects and network flow information
- Agent-less collection methods include SNMP, Syslog, WMI, Cisco SDEE, Checkpoint LEA, JDBC, VMWare VI-SDK, JMX, Telnet, SSH, network flow, and HTTP(S)
- Custom metrics can be collected via SNMP, WMI, JMX and JDBC
- Normalize data from multi-vendor, multi-technology devices into a common format
- XML-encoded event handling technology for flexible high throughput event parsing without requiring software updates. Add custom parsers for new device support by writing XML files
- More than 100 pre-defined XML parsers with more than 1000 parsed

attributes provide rich coverage of tier 1 and tier 2 IT vendors across virtually all technology categories

Dynamic User Identity and Location Mapping

- Associate IP addresses to machine names, MAC, switch VLAN Id, logged on user name and directory identity
- Identify mobile devices logging into network by device type (i.e. iPhone, iPad, Android, Blackberry) correlated with User Identity
- Append geo-location information (i.e. city, state, country, longitude and latitude) to every log and event using a system-provided and periodically updated geo-location database
- Identify user location based upon nearest WLAN access point, Controller, VPN Gateway and layer 2 switch port
- Associate primary logins to secondary logins to identify real user behind shared and administrative accounts
- Binds identity and location to events for real time correlation and post-event analysis
- Maintain an audit trail for each IP address identity and location mappings for historical analysis and compliance reporting

Event Search, Drilldown, and Robust Reporting

- Unified method to search events, logs, files and performance metrics across security, performance, availability and change management domains
- Real time search based on Google-like keywords and SQL-like structured queries on parsed event attributes
- Historical search with SQL-like filtering, result aggregation, and sorting
- Scalable parallel data-management architecture provides the ability to reduce search times by adding virtual appliances without any downtime
- Intuitive GUI simplifies search definition
- XML-based search and report definition enables sharing within user community
- Ability to trend search results identifies spikes, dips and anomalies
- Ability to convert search results into reports and dashboard widgets
- One-click recursive drill down for refining search criterion streamlines root-cause analysis
- Over 1500 customizable reports, categorized into device groups (such as network devices, servers, storage, and applications) and into functional groups (such as performance, availability, security, and change management)
- Ability to schedule a report to run at any time interval and period, and to be delivered via email and SMS
- Report results exportable to standard formats such as PDF and CSV

Real-Time Event Correlation, Statistical Profiling, Root-cause Analysis, and Alerting

- Unified method to predict security threats and IT operational issues by real-time cross-correlation of events and key performance metrics across security, performance, availability, and change management domains
- More than 250 built-in rules cover variety of scenarios spanning performance, availability, security, and change management
- Global cross-correlation using multiple AccelOps virtual appliances to handle unlimited events, logs, metrics and rules
- Create new rules or customize built-in rules using intuitive GUI
- Manage alert suppression and exceptions using rules GUI
- Rules can vary from simple thresholds to comprehensive patterns supporting full Boolean logic and allowing:
  - Sub-patterns connected in time dimension by operators such as AND, OR, FOLLOWED_BY, AND_NOT, and NOT_FOLLOWED_BY
  - Each sub-pattern can filter and apply aggregation operators such as AVG, MAX, MIN, COUNT and COUNT DISTINCT
  - Thresholds can be static or statistically derived from profiled data
- Statistical profiling to baseline network activity, system resource consumption, errors and user/service account activity
- User defined maintenance schedules ensure alerts are not sent out during maintenance windows
- Policy based notification handles enterprise grade incident management
- Alerts delivered via console, email, SNMP trap, XML push and SMS includes metadata such as host/user identity, location details. Alerts can also trigger customizable notification scripts.
- XML-based rule definition enables sharing within user community

Business Service Discovery, Mapping and Impact Analysis

- Ability to define a business service as a smart container of devices and applications serving specific business purpose speeds troubleshooting and problem resolution
- Wizard to create business services by choosing relevant devices and applications based on CMDB, topology and traffic flows
- Visualize business service components on the topology map
- Prioritize incidents by business service and assess service SLA by comparing against current metrics and trends

- Create reports and dashboards customized by business applications for specific departments and organizations within the enterprise.

Virtualization Monitoring

- Cross-correlates hardware, storage, VM, v-Switch, Guest Host/OS and application health, performance and incidents
- Interactive VM dashboard: ESX and VM vitals, relationships, metrics, configurations, trends, events and location
- Tracks new VMs as they are introduced and monitors for excessive VM migration across different physical machines
- Identifies VM contention and issues regarding respective hardware and storage performance and resource utilization
- Links virtual and physical resources and relationships to business and business services

Cloud Service Monitoring

- Monitor guest OS and applications deployed in an EC2 cloud by deploying an EC2 collector
- Monitor detailed system and application metrics and logs for cloud applications in fine grained time intervals
- Validate cloud SLAs, monitor malicious cloud activities, and trigger alerts for out-of-bounds conditions
- Combine on-premise SLAs with cloud SLAs for effective hybrid cloud monitoring

Multi-tenancy for Managed Service Provider Deployments

- Multi-tenant software architecture permits logical separation between various customer data while simultaneously sharing the same hardware
- Secure, customized alerts, reports, and visibility for each client customer
- Multi-tenancy allows enterprises to create secure partitioned business unit, departmental or geographical views for security, confidentiality, and compliance purposes

Role and Function-based Integrated Monitoring Dashboard

- Built-in unified summary dashboard for a consolidated overview of performance, availability and security metrics for devices and applications; grouped by specific IT functional groups or a defined business service
- Obtain more context by launching device and application level overview, and by drilling down into specific events and incidents
- Built-in performance, availability, security and change dashboards; device and application level dashboards
- Ability to customize any dashboard by adding reports and metrics
- In-memory database technology allows fast, near real time auto refresh of dashboard data for a large number of devices and metrics

Incident Management With Trouble Ticketing

- Create, open, assign, change status and close tickets from incidents
- Ability to add notes and attachments to tickets, as well as conduct an audit trail of activity regarding a ticket
- Reports on overall ticket activity including ticket audit trail details, and by business service or user
- Two-way integration with major help desk applications such as Remedy. Custom email based integration with all help desk applications

Change Management

- Monitor network device configurations for startup configuration change and difference between startup and running configuration
- Monitor servers for installed/uninstalled application, file/directory, running application status, and network port up/down changes
- Monitor directory service user/group membership changes
- Configurations versioned and archived in change management database (CMDB)
- Alert on unauthorized configuration change – tie in user identity and location to provide true user identity, contact information, IP address and workstation name
- Report on configuration change history by device or by business service

Security Information and Event Management (SIEM)

- Next generation SIEM that combines rich device support, scalable event collection, and global correlation with context from user identity, location, device, application configurations, availability, and performance metrics, to provide efficient, prioritized security analysis from a business service perspective
- Collect, parse, normalize, correlate and store security related logs from virtually all IT silos including:
  - Network activity logs from firewalls, routers, switches via network flow, VPN gateways, wireless LAN, Web/mail security gateways, and network IPS
  - Server operating system activity logs, host AV, and host IPS
  - Network infrastructure application logs: Domain Controllers, Authentication, DNS and DHCP servers, and vulnerability management servers
  - User application logs from web, application, and database servers
- Flexible XML-encoded-event-handling technology for high throughput event parsing without requiring software update. New device support can be added by writing XML files

- Profile network traffic flow and firewall logs to detect network services and baseline communication patterns by days-of-month, days-of-week, and by business and off-business hours
- Built-in security threat detections include:
  - Host scans, port scans, fixed-port host scans, denied scans, sudden increase/decrease of traffic from/to certain IPs, and other traffic anomalies from firewall and netflow logs
  - Network device and server admin logon anomalies – excessive authentication failures, repeated authentication failures, authentication failures during off business hours, and authentication failures from unusual IPs
  - Network access anomalies from VPN, domain controller and wireless logons
  - Web server and database access anomalies, as well as account lockouts, password scans and unusual failed logon patterns
  - Rogue workstations, PDAs, WLAN access points, etc. from DHCP logs
  - Botnets, mail viruses, worms, DDOS and other day zero malware by cross-correlating DNS, DHCP, web proxy logs and flow traffic
- Reduce network IPS false positives by comparing against installed patch information on servers
- Associate primary logins to secondary logins to identify real user behind administrative and shared account usage
- Associate IP addresses to machine names, MAC, switch VLAN Id, logged on user name and directory identity
- Prioritize incidents by business service with the ability to manage incidents via an integrated trouble ticket system
- Built-in, customizable security dashboard and over 200 security related reports
- Broad event/log source collection: Syslog, SNMP, WMI, Netflow V5/V9, HTTP(S), JDBC, Checkpoint LEA, Cisco SDEE, Telnet, SSH

Log Management and Compliance Automation

- Logs compressed and archived for the amount of time permitted by the storage sub-system to meet data retention requirements
- On-demand access to all raw events and incidents with retrieval duration, of at least one year determined by license
- Ability to archive events to off-line storage. Ability to bring back off-line data for real time analysis. Ability to provision off-line storage for multiple customers with per-customer storage requirements
- Built-in compliance rules/reports for PCI, SOX, HIPAA, ISO, COBIT, FISMA and GLBA serve as foundation for a variety of privacy and governance mandates

Performance and Availability Monitoring

- Comprehensive end-to-end performance monitoring of all infrastructure elements (including routers, switches, firewalls, load balancers and storage) in the path from user to application, and by combining system and end-user perspectives
- VMware cross-correlation: ESX, hardware, storage, and VM performance and health metrics
- Integration with security, change management, network flow analysis, and VM to quickly detect changes in application behavior
- Monitor system availability and performance via ping, hardware status, device uptime metrics, CPU, memory, disk, interface, process counts and thread counts
- Monitor process level performance including CPU, memory, disk activity and uptime
- Monitor detailed application level performance metrics for DNS, DHCP, SQL Server and Oracle databases, IIS and Apache web servers, app servers, and Microsoft Exchange
- Synthetic transaction monitoring of DNS, FTP/SCP, Generic TCP/UDP, ICMP, JDBC, LDAP, SMTP, IMAP4, POP3, POP3S, SMTP, SSH and Web — HTTP, HTTPS (Single and Multi-Step)
- Built-in and customizable rules to detect device, application, and business service health spanning multiple metrics
- Rules can be based on thresholds on aggregated metrics; thresholds can be static or dynamic based on statistical profiles of any metric
- Track performance and availability by business service. Track trends of metrics or of business service health and create reports
- Performance and availability data collected via SNMP, network flow, WMI, Telnet/SSH, JMX, HTTP(S), JDBC and VMware VI-SDK to cover wide range of applications, servers and network devices

Automated Remediation

- Ability to execute user-defined scripts when rules trigger – examples include
  - Shun IP addresses in firewalls and network IPS upon detecting malicious activity or excessive denies
  - Disable users from VPN gateways if logging from unauthorized locations
  - Disable users from WLANs upon detecting excessive traffic or policy violations

Inventory Management

- Collect network device and server inventory spanning all aspects of hardware and software information

- Hardware information includes specifications, license and serial numbers for bios, processor, memory, storage (local and remote), power supply, fan, RAID battery, etc.
- Software information includes items such as vendor, version, license information, usage for installed applications, installed patches, running/stopped services, and running processes
- Ability to associate inventory items such as department and user owner
- Automatically updated through repeated discovery at standard and user-defined intervals
- Ability to search and report on network inventory per device or group in both summary and detail

Administration

- Wizard-based implementation guide, online help and one-click upgrade
- Browser based GUI access with all communications secured via HTTPS
- Adobe Flex Web 2.0 implementation for desktop-like user experience
- Role based Access Control with user actions recorded via audit trail

Clustered Virtual Appliance Delivery

- Software on premise solution installed as a native virtual appliance running on VMware ESX or ESXi
- Deployable as a single, all-in-one virtual machine for simplicity or on a cluster of virtual machines for scalability
- Scale-out architecture permits unlimited event collection throughput with instant search and correlation performance enhancement by adding virtual machines to the cluster
- Redundancy achieved by a combination of application failover and virtualization failover ensuring high availability
- Built-in hybrid data management comprised of flat file and embedded PostgreSQL database for unlimited online data analysis; determined by the amount of VMware or NFS reference storage and the AccelOps' license

AccelOps Models and Installation Requirements

Security Information Event Management (SIEM)

- SIEM knowledgebase, event log management, real-time correlation, compliance management, identity access monitoring, change monitoring, netflow analysis, IDS filtering...
- Licensed by Events Per Second (EPS): 750, 1500, 4500, 7500, 10000, 25000

Performance / Availability Monitoring (PAM)

- Performance and SLA monitoring knowledgebase, change monitoring, VM management, network monitoring, business service management, performance monitoring...
- Licensed by Device Count: 10, 25, 100, 500,1000, 2500, 5000, 10000, Enterprise

AccelOps Foundation Module

- Discovery, CMDB, Visualization, Service Mapping, Cross-correlation Engine, Alerting, Dashboards, Identity, Incident Management, Search, Online Data Analysis. Licensed by Device Count: 250. 500, 1000, 2500, 5000, 10000, Enterprise

Foundation SP (Service Provider)

- Multi-tenancy, Consolidated Console, Multi-Site Management, Elastic Capacity. Licensed by Maximum Device Count: 250, 1000, 2500, 5000

AccelOps Model	Devices	Events Per Second	Host SW	Processor	Memory	Minimum Storage [1]
AO-VA-250	250	4500	VMWare ESX	Quad core, 3GHz, 64 bit	16GB	2.4TB
AO-VA-500	500	7500	VMWare ESX	Quad core, 3GHz, 64 bit	16GB	7.2TB
AO-VA-1000	1000	10000	VMWare ESX	Quad core, 3GHz, 64 bit	16GB	12TB
AO-VA-2500	2500	18000	VMWare ESX	Quad core, 3GHz, 64 bit	16GB	12TB
AO-VA-5000	5000	32000	VMWare ESX	2x Quad core, 3GHz, 64 bit	16GB	12TB
AO-VA-10000	10000	32000	VMWare ESX	2x Quad core, 3GHz, 64 bit	16GB	18TB
AO-Collector	N/A	N/A	VMWare ESX	Dual core, 2GHz, 64 bit	4GB	80GB

1 AccelOps virtual appliance can utilize any storage configured within VMWare ESX or can reference external NFS storage. The amount of storage listed is the amount typically required for one year of Online Data Access (ODA) and may vary depending upon device type and activity level. A license can be obtained to extend data retention and provide EPS elasticity to accommodate activity bursts.

AccelOps Supported Vendor and Device Sources

Antivirus
- Cisco CSA
- ESET Nod32
- McAfee EPO
- Sophos Endpoint Control
- Symantec Endpoint Protection
- Trend Micro IDF
- Trend Micro OfficeScan

App Server
- ASP.NET
- GlassFish
- Redhat JBOSS
- Tomcat

Authentication Servers
- Cisco ACS
- Juniper Steel-Belted RADIUS
- Microsoft IAS

Backup
- Zenith ARCA

Blade Servers
- Cisco UCS

Cloud Services
- Amazon EC2

Database
- Microsoft SQL Server
- MySQL
- Oracle Database Server
- PostgreSQL

Directory
- Microsoft AD 2000, 2003, 2008

DNS/DHCP Servers
- BIND DNS
- InfoBlox DNS/DHCP
- Linux DHCP
- Microsoft DHCP 2003, 2008
- Microsoft DNS 2003, 2008

Email
- Exchange
- Postfix Mail Server
- Sendmail

Environmental
- APC UPS
- Liebert UPS, HVAC, FPC
- NetBotz

External Monitoring
- Nagios

File Monitoring
- Linux
- Windows

Firewall
- Astaro
- CheckPoint FW-1, Provider-1
- Checkpoint VSX
- Cisco ASA, IOS
- Cisco FWSM, PIX
- Fortinet
- Juniper SSG, ISG
- Linux ipchains
- McAfee Enterprise (Sidewinder)
- Microsoft ISA
- Palo Alto Networks
- SonicWALL SonicOS
- WatchGuard

Hardware Monitoring
- Dell servers
- HP servers
- IBM servers
- Network devices
- Storage devices

Host OS
- HP-UX
- IBM AIX
- IBM OS/400
- CentOS
- Fedora
- Redhat
- SUSE
- SUN Solaris, SunOS
- Windows 2000, 2003, 2008

Internet Security Gateways
- Astaro Secure Gateway
- Barracuda Spam Firewall
- Blue Coat ProxySG
- Cisco IronPort
- McAfee Web Gateway
- Microsoft ISA Server
- Squid
- Untangle Secure Gateway
- WebSense MailFilter
- WebSense WebFilter

IPS
- Checkpoint
- Cisco CSA, IPS
- FireEye
- ForeScout
- Juniper IDP
- McAFee Intrushield
- Snort IPS
- TippingPoint IPS

Load Balancers
- F5

Network Flow
- netflow v5, v9

Remote Desktop
- Citrix ICA

Router/Switch
- Alcatel-Lucent TiMOS, AOS
- Brocade Foundry IronWare
- Cisco CatOS, IOS,
- Cisco MDS
- Cisco NX-OS
- ExtremeWare XOS
- H3C Comware
- HP ProCurve
- Huawei VRP
- Juniper Junos
- Nortel ERS, Passport

Storage
- Dell EqualLogic
- EMC Clariion
- Isilon OneFS
- NetApp Data ONTAP
- Host attached storage

Synthetic Transaction Monitoring
- Web – HTTP/HTTPS
- DNS
- FTP/SCP
- Generic TCP/UDP
- ICMP
- IMAP4
- JDBC
- LDAP
- POP3
- POP3S
- SMTP
- SOAP
- SSH
- Telnet/SSH

Syslog
- Syslog-ng

Terminal Servers
- Microsoft ICA

Unified Threat Management (UTM)
- SonicWALL
- Fortinet

Virtualization
- VMWare ESX, ESXi, vSphere, vCenter

VoIP Servers
- Cisco Call Manager
- Cisco IOS IPSLA
- Cisco CBQoS

VPN Gateway
- Cisco ASA VPN3000
- Juniper SSL VPN
- Microsoft PPTP/L2TP
- SonicWALL Aventail

Vulnerability Scanners
- nCircle
- QualysGuard
- Rapid7 Nexpose
- Tenable Nessus

WAN Accelerators
Riverbed Steelhead

Web Server
- Apache Webserver
- Microsoft IIS for Windows 2000, 2003, 2008
- Nginx Webserver

Wireless
- Aruba ArubaOS
- Cisco WLAN
- NetMotion Mobility XE

AccelOps, Inc.
2901 Tasman Drive, Suite 100
Santa Clara, CA 95054, USA

Web: www.accelops.com
Tel: 1 (408) 490-0903
Email: sales@accelops.com