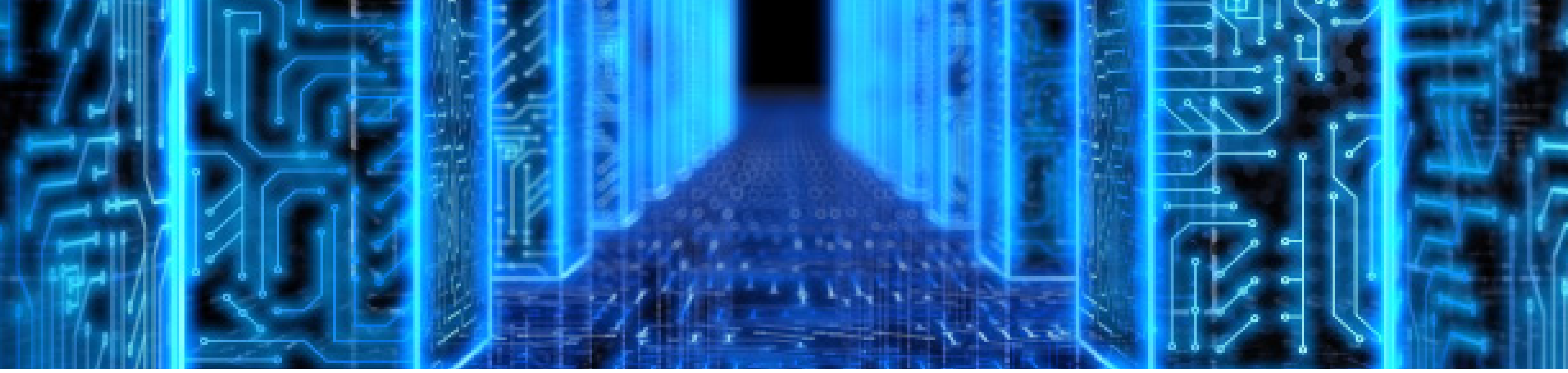


CASE STUDY

**Customer:** Denali Alaskan Federal Credit Union

**Industry:** Financial Services

**Results with AccelOps:**

- Cross-correlation, online data retention and SOC/NOC interoperability that address today's security requirements
- Scaled operational visibility and more automated compliance controls at a lower total cost of ownership
- Management and better use of increased audit and operational data
- Integrated log management, SIEM, flow analysis, configuration and performance monitoring

# Denali Alaskan Federal Credit Union Chooses AccelOps to Scale Operational Visibility, Gain More Automated Compliance Controls at Lower TCO

Denali Alaskan Federal Credit Union is the third largest credit union in Alaska with assets in excess of $480 million and 18 branches in all major communities. The full-service financial institution offers core credit union banking, as well as investment, mortgage, business lending and insurance services. It is a federally chartered financial institution serving more than 58,000 members.

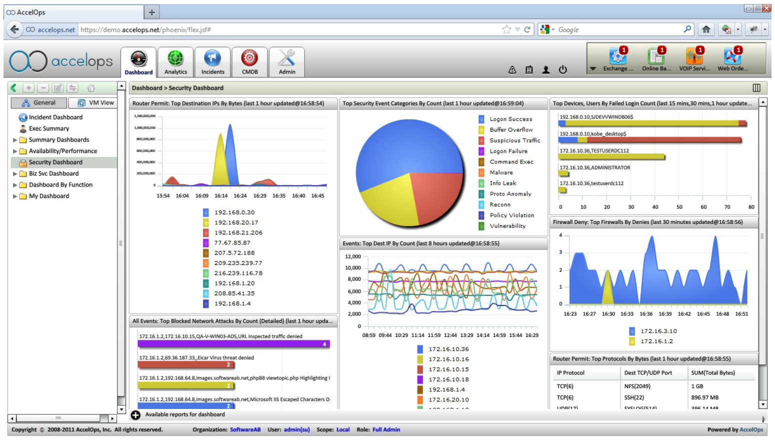
## IT Challenges

Denali Alaskan Federal Credit Union's primary challenge was to expand its Security Information and Event Management (SIEM) capacity and automate compliance processes to address National Credit Union Administration and Federal Financial Institutions Examination Council standards, as well as Gramm-Leach-Bliley (GLBA) requirements and standards set by the Payment Card Industry (PCI). In addition, the credit union, which had previously used LogRhythm, was seeking to scale its operational visibility and gain more automated compliance controls at a lower total cost of ownership.

"Organizations must defend against more complex internal and external threats, manage fraud and compliance risks, and respond to incidents faster and according to business impact," said Richard Stiennon, security expert and chief research analyst at IT-Harvest. "To accomplish this, infosec professionals require broader and more intelligent operational visibility."

## The Solution

Denali Alaskan Federal Credit Union selected AccelOps for its integrated network security, log, identity and configuration monitoring. Using AccelOps, the credit union is able to consolidate, monitor, analyze, report and retain volumes of log and event data. The solution offers real-time correlation, historical forensic analysis and compliance reporting without requiring deployment of software agents.



172.16.1.2,172.16.10.15,QA-V-WIN03-ADS,URL inspected traffic denied

172.16.1.2,69.36.187.33,,Eicar Virus threat denied

172.16.1.2,192.168.64.8,images.softwareab.net,phpBB viewtopic.php Highlighting I

172.16.1.2,192.168.64.8,images.softwareab.net,Microsoft IIS Escaped Characters D

Router Permit: Top Protocols By Bytes (last 1 hour updated@16:58:55)

| IP Protocol | Dest TCP/UDP Port | SUM(Total Bytes) |
|---|---|---|
| TCP(6) | NFS(2049) | 1 GB |
| TCP(6) | SSH(22) | 896.97 MB |

Copyright © 2008-2011 AccelOps, Inc. All rights reserved. Organization: SoftwareAB User: admin(su) Scope: Local Role: Full Admin Powered by AccelOps

*AccelOps Dashboard*

"AccelOps not only provides the necessary built-in security and compliance knowledgebase, but offers innovations in cross-correlation, online data retention and SOC/NOC interoperability that address today's security requirements," Stiennon said.

Denali Alaskan joins many other customers who are migrating from conventional log management and SIEM systems to AccelOps' all-in-one application that provides next-gen security (SIEM), performance and availability monitoring that works across traditional data centers, and private and hybrid clouds.

Many organizations are looking beyond conventional SIEM approaches to address:

- SOC/NOC interoperability, in which cross-correlating a broader set of operational controls yields 360-degree insight and root-cause analysis of value to all IT functions.
- Expensive, disparate single-domain tools.
- The excessive time and resources expended to support the myriad of incident response, audit and operational reporting activities.
- The administrative burden and cost to implement, maintain and scale SIEM products.

## The Results

"We knew that we needed a more capable security and log management approach that could help us manage and make better use of increased audit and operational data," said Keith Bennett, vice president of information technology at Denali Alaskan Federal Credit Union. "AccelOps was straightforward to implement, administer and scale, with immediate value for my security and network staff. The virtual appliance package with combined log management, SIEM, flow analysis, configuration and performance monitoring offers demonstrable advantages."

AccelOps goes beyond conventional SIEM approaches by providing a single pane of glass that cross-correlates security and performance operational data across an organization's servers, storage, network, security, users and applications both on-premise and in the cloud.

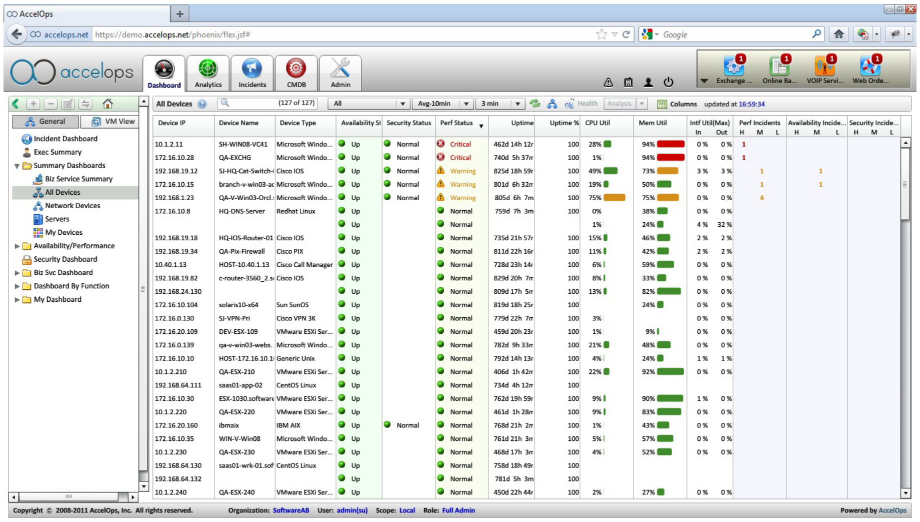
Key capabilities that figured prominently in Denali Alaskan's selection of AccelOps were:

- Compliance: Integrated network security, configuration and identity monitoring with built-in rules and reports mapped to leading compliance frameworks.
- Usability: Ease of use and extensive incident, search and reporting analytics.
- Network flow and IDS integration: Network behavior analysis and automated IDS false positive filtering to pinpoint sophisticated threats and reduce noise.
- Administration and Scale: Simpler deployment and maintenance with the means to scale on demand by leveraging VMware virtual appliance and external storage.
- Next-Gen SIEM: Automated Configuration Management Database (CMDB), performance monitoring and service mapping for greater oversight, collaboration and incident prioritization by business impact.

*"AccelOps was straightforward to implement, administer and scale, with immediate value for my security and network staff. The virtual appliance package with combined log management, SIEM, flow analysis, configuration and performance monitoring offers demonstrable advantages."*

Keith Bennett,
Vice President
of Information
Technology, Denali
Alaskan Federal
Credit Union

> *“AccelOps not only provides the necessary built-in security and compliance knowledgebase, but offers innovations in cross-correlation, online data retention and SOC/NOC interoperability that address today’s security requirements.”*
>
> Richard Stiennon, Security Expert
> and Chief Research Analyst,
> IT-Harvest



updated at 16:59:34

| Device IP | Device Name | Device Type | Availability St | Security Status | Perf Status | Uptime | Uptime % | CPU Util | Mem Util | Intf Util(Max) | | Perf Incidents | | | Availability Incide... | | | Security Incide... | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | In | Out | H | M | L | H | M | L | H | M | L |
| 10.1.2.11 | SH-WIN08-VC41 | Microsoft Windo... | Up | Normal | Critical | 462d 14h 12r | 100 | 28% | 94% | 0 % | 0 % | 1 | | | | | | | | |
| 172.16.10.28 | QA-EXCHG | Microsoft Windo... | Up | Normal | Critical | 740d 5h 37r | 100 | 1% | 94% | 0 % | 0 % | 1 | | | | | | | | |
| 192.168.19.12 | SJ-HQ-Cat-Switch-( | Cisco IOS | Up | Normal | Warning | 825d 18h 59r | 100 | 49% | 73% | 3 % | 3 % | | 1 | | | 1 | | | | |
| 172.16.10.15 | branch-v-win03-ac | Microsoft Windo... | Up | Normal | Warning | 801d 6h 32r | 100 | 19% | 50% | 0 % | 0 % | | 1 | | | 1 | | | | |
| 192.168.1.23 | QA-V-Win03-Orcl.: | Microsoft Windo... | Up | Normal | Warning | 805d 6h 7m | 100 | 75% | 75% | 0 % | 0 % | | 4 | | | | | | | |
| 172.16.10.8 | HQ-DNS-Server | Redhat Linux | Up | | Normal | 759d 7h 3m | 100 | 0% | 38% | 0 % | 0 % | | | | | | | | | |
| | | | Up | | Normal | | | 1% | 24% | 4 % | 32 % | | | | | | | | | |
| 192.168.19.18 | HQ-IOS-Router-01 | Cisco IOS | Up | | Normal | 735d 21h 57r | 100 | 15% | 46% | 2 % | 2 % | | | | | | | | | |
| 192.168.19.34 | QA-Pix-Firewall | Cisco PIX | Up | | Normal | 811d 22h 16r | 100 | 11% | 42% | 2 % | 2 % | | | | | | | | | |
| 10.40.1.13 | HOST-10.40.1.13 | Cisco Call Manager | Up | | Normal | 728d 23h 14r | 100 | 6% | 59% | 0 % | 0 % | | | | | | | | | |
| 192.168.19.82 | c-router-3560_2.s | Cisco IOS | Up | | Normal | 829d 20h 7r | 100 | 8% | 33% | 0 % | 0 % | | | | | | | | | |
| 192.168.24.130 | | | Up | | Normal | 809d 17h 5r | 100 | 13% | 82% | 0 % | 0 % | | | | | | | | | |
| 172.16.10.104 | solaris10-x64 | Sun SunOS | Up | | Normal | 819d 18h 25r | 100 | | 24% | 0 % | 0 % | | | | | | | | | |
| 172.16.0.130 | SJ-VPN-Pri | Cisco VPN 3K | Up | | Normal | 779d 22h 7r | 100 | 3% | | 0 % | 0 % | | | | | | | | | |
| 172.16.20.109 | DEV-ESX-109 | VMware ESXi Ser... | Up | | Normal | 459d 20h 23r | 100 | 1% | 9% | 0 % | 0 % | | | | | | | | | |
| 172.16.0.139 | qa-v-win03-webs. | Microsoft Windo... | Up | | Normal | 782d 9h 33r | 100 | 21% | 48% | 0 % | 0 % | | | | | | | | | |
| 172.16.10.10 | HOST-172.16.10.1( | Generic Unix | Up | | Normal | 792d 14h 13r | 100 | 4% | 24% | 1 % | 1 % | | | | | | | | | |
| 10.1.2.210 | QA-ESX-210 | VMware ESXi Ser... | Up | | Normal | 406d 1h 42r | 100 | 22% | 92% | 0 % | 0 % | | | | | | | | | |
| 192.168.64.111 | saas01-app-02 | CentOS Linux | Up | | Normal | 734d 4h 12r | 100 | | | | | | | | | | | | | |
| 172.16.10.30 | ESX-1030.software | VMware ESXi Ser... | Up | | Normal | 762d 19h 59r | 100 | 9% | 90% | 1 % | 0 % | | | | | | | | | |
| 10.1.2.220 | QA-ESX-220 | VMware ESXi Ser... | Up | | Normal | 461d 1h 28r | 100 | 9% | 83% | 0 % | 0 % | | | | | | | | | |
| 172.16.20.160 | ibmaix | IBM AIX | Up | Normal | Normal | 768d 21h 2r | 100 | 1% | 43% | 0 % | 0 % | | | | | | | | | |
| 172.16.10.35 | WIN-V-Win08 | Microsoft Windo... | Up | | Normal | 761d 21h 3r | 100 | 5% | 57% | 0 % | 0 % | | | | | | | | | |
| 10.1.2.230 | QA-ESX-230 | VMware ESXi Ser... | Up | | Normal | 468d 17h 3r | 100 | 4% | 52% | 0 % | 0 % | | | | | | | | | |
| 192.168.64.130 | saas01-wrk-01.sof | CentOS Linux | Up | | Normal | 758d 18h 49r | 100 | | | | | | | | | | | | | |
| 192.168.64.132 | | | Up | | Normal | 781d 5h 3m | 100 | | | | | | | | | | | | | |
| 10.1.2.240 | QA-ESX-240 | VMware ESXi Ser... | Up | | Normal | 450d 22h 44r | 100 | 2% | 27% | 0 % | 0 % | | | | | | | | | |

Copyright © 2008-2011 AccelOps, Inc. All rights reserved. Organization: SoftwareAB User: admin(su) Scope: Local Role: Full Admin Powered by AccelOps

*AccelOps Report*

## About AccelOps

AccelOps provides a new generation of integrated security, performance and availability monitoring software for today’s dynamic, virtualized data centers. Based on patented distributed real-time analytics technology, AccelOps automatically analyzes and makes sense of behavior patterns spanning server, storage, network, security, users, and applications to rapidly detect and resolve problems. AccelOps works across traditional data centers as well as private and hybrid clouds. The software-only application runs on a VMware ESX or ESXi virtual appliance and scales seamlessly by adding additional VMs to a cluster. Its unmatched delivery of real-time, proactive security and operational intelligence allows organizations to be more responsive and competitive as they expand the IT capabilities that underpin their business.

**FREE TRIAL DOWNLOAD**
www.accelops.com/download

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