

Příloha č. 1 – Minimální seznam podporovaných zdrojů logů

<b>Minimální seznam podporovaných zdrojů logů</b>
Apache httpd
Apache Tomcat
Brocade FC switches
<b>ArcSight CEF format all sources</b>
Cisco ASA
Cisco Firepower
Cisco IOS
Cisco IronPort
Cisco Nexus
Cisco SMB
Cisco WLC
CompuNet GAMA (on request)
Dell Force10
Dell iDrac (Server OoB management)
Dell PowerConnect
Dell SonicWALL
Dell W-series WiFi
FlowMon
FortiAuthenticator
FortiDDoS
Fortigate
FortiGate-Lite (performance optimized)
FortiMail
FortiManager
FreeRADIUS
<b>Qradar LEEF format all sources</b>
HAProxy (structured rfc5425 logformat)
HPE Aruba Instant AP (WLAN)
HPE Aruba Mobility Controller (WLAN)
HPE iLo 4 (Server OoB management)
HPE IMC
HPE routers
HPE switches Procurve OS
HPE switches Comware OS
HPE Comware WLAN
ISC BIND
ISC DHCP
ISC DHCPD
<b>JSON format all sources</b>
Linux Cron
Linux Freeradius
Linux Iptables

Příloha č. 1 – Minimální seznam podporovaných zdrojů logů

Linux Postfix
LOGmanager
Mikrotik
Microsoft Exchange log
Microsoft SharePoint
Microsoft SQL
Microsoft Windows DHCP log
Microsoft Windows DNS debug log
Microsoft Windows Firewall (optimized for performance)
Microsoft Windows IIS
OpenSSH server
Oracle DB
PostgreSQL
SAP
<b>RFC5425 format all sources</b>
Synology NAS DSM
TrendMicro DeepDiscovery
TrendMicro TippingPoint NG-IPS
VMware
Windows - any logs from Event Viewer
Windows - any text log from file