CenturyLink Technology Solutions

CenturyLink Technology Solutions Service Guide

Log Management Service

This Service Guide (“SG”) sets forth a description of CenturyLink Log Management Service (“Service”) offerings including technical details and additional requirements or terms, if any. This SG is subject to and incorporated into the Master Service Agreement and Service Schedule between the parties. The specific details of the Service ordered by Customer will be set forth on the relevant Service Order.

Version	Previous	Section Modified	Date
SEC-20140430-SG-LogManagementService	SEC-20091208-External-SSG-GL-Log_Management_Service	Rebrand	April 30, 2014

CenturyLink Technology Solutions
www.centurylink.com/technology

Town & Country, MO 63017
Office: 314.628.7000

Table of Contents

Service Description

The Service provides a log management service, including hardware, software, installation, 24/7 monitoring, alerting, and support. The Service includes a dedicated, managed log management appliance (CenturyLink Equipment), from which customer log traffic is sent via an encrypted session to the centralized CenturyLink log management infrastructure for processing and archival.

Service Options

This CenturyLink Service Guide pertains to the following services,

Location	Tier	Installation
Service in IDC	Small	Log Management Set-up, Installation, Configuration -Small
	Large	Log Management Set-up, Installation, Configuration -Large
Services at Customer Premises	Small	Log Management Set-up, Installation, Configuration -Small
	Large	Log Management Set-up, Installation, Configuration -Small

Systems Supported:

A complete listing of supported devices is available upon request. The Log Management service will support devices that utilize

- syslog
- Check Point firewall logs
- Windows OS logging
- UNIX OS logging Potentially non-supported logging formats will be reviewed for compatibility with the service prior to log collection.

Installation

- CenturyLink will provision the log management appliance and work with the Customer to set up and configure the service.
- CenturyLink IDC implementations will include a connection to the CenturyLink internal management network to allow for out-of-band device administration.
- CenturyLink will work with the Customer to determine their logging rate, as measured in messages per second.
- CenturyLink will provide customers with log source configuration guidelines for devices that are supported within the Service. Configuration of the log source will be the Customer's responsibility for non-CenturyLink-managed devices. A list of supported devices is available upon request.

Configuration

- CenturyLink will configure the Service to support a standard defined set of alert rules, with up to twenty (20) additional customized alert rules. Support of additional alert rules will be considered on an as requested basis.
- Includes set-up of CenturyLink-defined reporting.
- Includes set-up of Customer-defined reporting.

Not Included in Service

The following are not included in the Service offering,

- Direct access to network security engineering. All initial contact goes through the CenturyLink Support Center.
- Log file archive retrievals for time periods beyond the prior 12 months.
- Support of log sources that are not on the accepted list of supported devices.
- CenturyLink configuration of customer-managed log sources.
- GiGE fiber cable connections into the log management appliance.

Optional Security Services

The following Security-related services are available through CenturyLink's Professional Services organization, and are not included with the Service:

- Application Security Review
- Network Penetration Testing
- Risk Assessment Services
- Security Architecture & Design
- Security Account Manager (SAM) Service
- Security Policy Creation & Documentation

For more details regarding the services outlined above, please contact your CenturyLink Account Executive

Upgrades

CENTURYLINK may periodically upgrade the log management software so the latest versions are in operation. If CENTURYLINK determines that an upgrade is necessary, CENTURYLINK will schedule a time to make necessary changes, preferably during the normally scheduled Data Center maintenance window. Customer will be notified by email or phone at least 10 days in advance of the maintenance. Completion of scheduled maintenance is required, or CENTURYLINK'S obligation to provide this service in accordance with this CENTURYLINK Service Guide will be suspended until Customer grants CENTURYLINK the access CENTURYLINK requires to make such changes. If CENTURYLINK determines that an emergency security change is required, CENTURYLINK will make the change as quickly as possible. CENTURYLINK will make commercially reasonable attempts to contact the Customer prior to making said change.

Monitoring

ICMP (e.g., ping) monitoring of the log management appliance to determine system availability (24/7).

Reporting

CenturyLink will provide reporting on predefined categories for supported devices via a dedicated log management appliance. This appliance provides for the generation of customizable reports, and is managed by the Customer. During installation of the Service, CenturyLink will make the dedicated log management appliance available to the customer, and work with Customer personnel to educate them on report setup and generation.

- The Customer may also request that CenturyLink configure customized reports. These requests are accommodated via the Customer's submitting a change request to the CenturyLink Support Center.
- Reports may be optionally distributed to a Customer-provided email address.
- Specific reports generated are dependent on customer device settings and log levels, but may include the following:
- Firewall policy change report.
- Firewall traffic besides HTTP / SSL / SSH.
- Update activities on Windows servers.
- Account activities on Windows servers.
- Account activities on UNIX servers.
- Unauthorized logins.

Frequency

- Views will be available in 12, 24, 48 hours and one calendar day, one week, one month timeframes
- Reports will be available based on log data from the preceding 90 days.
- Raw log files will be available for a 90-day period on-line.

Fault reporting and service restoration

- Suspected faults on the Service should be reported to CenturyLink at the telephone number provided to the Customer for this purpose.
- To diagnose and resolve suspected faults, CenturyLink requires certain information when the problem is first reported. This will normally include:

Required Information
The CenturyLink references for the circuit(s) and/or any other part of a service thought to be affected
Symptoms of the problem
Details if any tests carried out in attempting to isolate the problem
Whether affected services can be taken out of service for testing, if necessary
The name and telephone number of the person reporting the fault

Customer Installation Requirements

- Customer must provide CenturyLink with a network topology of their existing network.
- Internet accessibility, as log transit to the CenturyLink infrastructure is sent encrypted and compressed utilizing the customer provided Internet connection.
- Installation of the Log Management service within a CenturyLink-managed environment will include 1U of rack space and power provided by CenturyLink. Installations not performed within the CenturyLink-managed environment will require Customer to provide 1U of rack space and power necessary for the Log Management appliance.
- Installation of the Log Management service within a CenturyLink-managed environment will include (1) VLAN, (1) 10/100/1000 connection to the Log Management appliance. Installations not performed within the CenturyLink-managed environment will require a customer-provided 10/100/1000 network connection into the customer switching infrastructure. For CenturyLink Managed Hosting environments any Ports and VLANs in addition to those included in the standard CenturyLink design shall be subject to incremental charges as set forth in the relevant Order Form. Any Port or VLAN requested by Customer after the initial installation of the Service shall also be subject to additional, incremental charges.
- Customer must provide IP addresses for all network connections to the shared log management infrastructure. For fully managed environments, CenturyLink will provide IP addresses.
- The Customer will, using CenturyLink's standard procedures, notify CenturyLink of the initial and later changes to the network information to be configured by CenturyLink within the Service.
- CenturyLink strongly recommends that the log management appliance be installed on a protected network, behind a sufficiently configured firewall that will help protect the appliance from both external and internal attacks and wrongful entries.
- Implementation of the log management appliance may require firewall rules be opened to allow for communication of log files from isolated network segments. In the event that this design conflicts with the Customer's security policy, an additional log management appliance may be required, at an additional cost to the Customer.
- For service deployments outside of the CenturyLink IDC, the Customer will arrange and pay for a standard (POTS) telephone line (with direct inward dialing) for each Customer site to enable CenturyLink to perform remote network management functions on the log management appliance. CenturyLink will not be responsible for any problems related to the delivery of the Log Management service on Customer Premises if this telephone line is not available or if is not functioning properly at all times.

Customer Responsibilities

- Customer must comply with all of its responsibilities under this CenturyLink Service Guide or CenturyLink's obligation to provide this service in accordance with this CenturyLink Service Guide will be suspended until Customer does so.
- Customer will have the responsibility to investigate alerts provided to them as part of the Service, including CenturyLink-defined and customer-defined alerting.
- Since the Service — as with all security systems — has potential vulnerabilities, the Customer should consider the Service as just one tool to be used as part of an overall security strategy, and not as a total solution.
- The Customer will not instruct or permit any other party to take any actions that would reduce the effectiveness of the Log Management Appliance.

- If the Customer's provider has an ACL on the Internet connections, the Customer must allow CenturyLink access for management and monitoring.
- Customer will have responsibility to identify each logging source from which log files are to be collected.
- Customer will have responsibility to configure each logging source that is not CenturyLink- managed.
- For service deployments at customer premise sites, the Customer will have responsibility for the physical network installation of the log management appliance. Onsite installation services for deployments can be provided by CenturyLink, at an additional cost to the Customer.
- Customer has sole and exclusive responsibility for any sensitive payload contained within log data.

Maintenance and Support

- 24/7 support for Log Management problem resolution and Customer inquiries.
- CenturyLink will allow real-time access to log file data for a maximum of (90) ninety days, to be accessed via a dedicated log management appliance.
- CenturyLink will archive log data offsite for a maximum of (12) twelve months.
- CenturyLink will support Customer requests to add additional logging sources for log collection on CenturyLink-supported devices. Customer will be responsible for requesting the additions and configuring the logging source.
- CenturyLink will provide Customer's hardware maintenance, which is available with a next business day response time
- Configuration consistency and change accountability requires that all IMS passwords will be managed by CenturyLink. Customer will not have access to firewall passwords or be able to make direct changes to their configurations. Customer must request changes by first contacting the CenturyLink Response Center. Customer must provide complete log-in credentials to the CenturyLink Response Center when requesting changes. These log-in credentials are the same as those used to log into CenturyLink's secure Web- based interface. See the Response Times section below for more information on response times.

Response Times

CenturyLink's response notification for this Service is defined as follows,

Response Event	Response Time and Procedure
Critical Alarm	CenturyLink personnel will review critical alerts within 15 minutes and will attempt to notify the Customer within 60 minutes, by telephone, pager or electronic mail, as specified in the Customer's escalation procedure.
Configuration, Report Creation Request and Policy Change Request	CenturyLink will respond to routine configuration and policy change requests within 12 business hours.
Fault reaction time to Service outage	CenturyLink opens a Service Request and begins work on issue within 15 minutes of Customer call or problem detection. CenturyLink updates Customer every 2 hours via Customer's preferred method (e.g. phone, email, page) until issue is resolved or Customer declines updates.
Restoration of Log data aged	CenturyLink personnel will begin restoration of log files within 6 hours of customer request.

Response Event	Response Time and Procedure
>90 days	
Addition of new logging device	CenturyLink personnel will begin configuration within 24 business hours.

Level of Service

CenturyLink will supply hardware and software appropriate to the level of service purchased. Available service levels are,

Service Tier	Hardware-Dedicated Log Management Appliance	Alerting - CenturyLink will configure Service to support a standard defined set of alert rules
Small	up to 500 messages per second.	up to twenty (20) customized alert rules.
Large	up to 1500 messages per second.	up to twenty (20) customized alert rules.

Additional Service Requirements

Response Times SLA

In the event that CenturyLink is unable to provide service within the “Response Time” windows outlined above, the Customer’s sole and exclusive remedy shall be a service credit in the amount of three percent (3%) of the affected service MRC for each response time failure.

In no event will the credits accrued in any single month exceed, in the aggregate across all response time goals and incidents, thirty percent (30%) of the invoice amount for the affected service.

CenturyLink’s obligation to meet stated Response Times will not apply to,

- any problem caused by or associated with the Customer’s failure to meet specified Customer Requirements
- underlying Internet access service
- any security tests.

Availability SLA

Target availability for the Log Management Service is 99.99%, measured on a calendar month basis.

Availability is calculated by dividing the number of minutes of unscheduled downtime in a calendar month by the total number of minutes in that calendar month.

In the event that the Service does not meet the Availability target, the Customer’s sole and exclusive remedy shall be a service credit in an amount determined in accordance with the following table. In no event will the credits accrued in

any single month exceed, in the aggregate across all response time goals and incidents, fifty percent (50%) of the invoice amount for the affected service.

Level	Commitment Attainment	Service Credit (% of MRC for Affected Service)
Level 1	99.99% > Availability > 99.75%	10%
Level 2	99.75% ≥ Availability > 99.5%	20%
Level 3	99.5% ≥ Availability > 99.0%	35%
Level 4	Availability < 99.0%	50%

SLA Process

Customer must request any credit due hereunder within 30 days of the conclusion of the month in which it accrues. Customer waives any right to credits not requested within this 30-day period. Credits will be issued once validated by CenturyLink and applied toward the invoice which Customer receives no later than two months in which the credit accrued.

The Customer will not be entitled to receive a credit if: a. Customer has violated the CenturyLink Acceptable Use Policy (AUP) and such violation results in the suspension, interruption, or termination of the Services; b. Customer is in breach or default under any provisions of the Agreement and beyond the applicable cure period at the time the Downtime occurred.

The credits set forth herein are not cumulative and in no event will the credits accrued in any calendar month exceed, in the aggregate across all events, fifty percent (50%) of the MRC for the affected Service in the applicable calendar month.

General Service Requirements

If any third party software, including any corresponding documentation, is provided to Customer by CenturyLink in connection with the Service, Customer agrees to use such third party software strictly in accordance with all applicable licensing terms and conditions. CenturyLink makes no representations or warranties whatsoever with regard to such third party software. With respect to such software, Customer shall,

- Use such software in a machine readable format and only with the Service;
- Not in any way transfer, modify or copy the software except as part of the Service; and
- Not in any way hide, obscure, eliminate or modify any proprietary notice which appears on or in part of the Service.

Customer shall,

- Provide CenturyLink with sufficient system passwords, privileges and access to allow CenturyLink to install, configure, monitor and modify the Service.
- Not attempt (nor instruct or allow others to attempt) any testing, assessment, circumvention or other evaluation or interference with any Service without the prior written consent of CenturyLink.

- Notify CenturyLink at least 5 business days in advance of any changes that may affect the applicable Service (e.g., infrastructure, network topology changes)
- purchase and maintain a reliable, stable and always-on, high speed connection to the public Internet (i.e., DSL, T1, cable modem etc. -- a dial-up connection is not sufficient) and/or a standard (POTS) telephone line (with direct inward dialing) for each Customer Site to enable CenturyLink to perform remote network management functions.
- Designate and maintain a Customer Contact during the Service Term (including current contact information). "Customer Contact" means an English-speaking technical point of contact available 24 x 7 with sufficient knowledge, authority and access to address configuration issues, event notifications, system or infrastructure modifications and authentication of applicable CenturyLink systems.
- For CenturyLink Managed Hosting environments any Ports and VLANs in addition to those included in the standard CenturyLink design shall be subject to incremental charges as set forth in the relevant Order Form. Any Port or VLAN requested by Customer after the initial installation of the Service shall also be subject to additional, incremental charges. Provision of the Service is subject to Customer's compliance with this Section.

CenturyLink may manage all system administration passwords, including root level access, and may do so exclusively. In such case, Customer will not have access to system passwords nor be able to make changes to the system configurations and must instead submit change requests to CenturyLink.

CenturyLink may require access to Customer's staging environment that matches production configuration in order to test configuration stability prior to implementing software changes. A successful test on the staging system does not guarantee success on the production system. The Services do not include the development of a comprehensive change control process. There may be incompatibilities between a Service and particular Customer environments which cannot be resolved. In such cases, CenturyLink reserves the right to withdraw the Service from those particular environments, but only to the extent necessary to resolve the incompatibility and without modifying either party's obligations with regard to unaffected environments.

Customer may incur additional charges if:

- Customer impairs the Service;
- CenturyLink dispatches a technician to a Customer Site and the technician is unable to complete the work because Customer was not available when the technician arrived; or
- Customer incurs three false alarms in a month; in which case, Customer will pay a $300 false alarm fee, plus an additional fee for each additional false alarm during that month (except where CenturyLink provides the Internet connection). Customer may request that CenturyLink discontinue Service monitoring in order to avoid false alarm fees; provided, however, CenturyLink shall have no further monitoring obligations whatsoever with regard to the affected Service. CenturyLink may require the purchase of Incident Response ("IR") Services, which consist of CenturyLink personnel responding to security events impacting Customer. IR services are limited to response and mitigation of incidents and do not include ongoing or long-term security consulting, which are subject to additional terms and charges.

If a Service requires reconfiguration or retuning for any reason, including reducing false positives and nuisance alerts, CenturyLink will contact Customer, if necessary, to schedule the activity (typically during normal maintenance

windows) and Customer agrees to cooperate with CenturyLink to schedule such activity. If CenturyLink determines that an emergency security change is required, CenturyLink will make the changes deemed necessary as soon as reasonably possible and will notify the Customer of the changes as soon as practicable.

CenturyLink does not represent or warrant that the CenturyLink Equipment or the Service will be uninterrupted or error-free; will detect or generate an alert for every security event that may be recorded in customer logs; or meets any particular data security standard.