Skillsoft's Infrastructure and Security:

A Technical Overview

Mark Townsend, Co-Chief Product Officer, Skillsoft
Edi Feldman, Senior Director, Technical Services, Skillsoft

September 2013

Introduction

Skillsoft offers a wide range of training products including its hosted learning management system (LMS), Skillport®. This document provides details of design, development, maintenance and support practices for Skillport and other Skillsoft-hosted solutions. For additional technology or security details, or to answer any questions related to the information in this document, please contact your Skillsoft account executive to schedule a call with the appropriate Skillsoft staff.

Table of Contents

Skillport

Skillport is a full-featured, web-based LMS providing customers with traditional LMS features and full access to the broad range of Skillsoft training content including courses, videos, electronic books and more. As a fully-hosted, software-as-a-service product, Skillsoft manages all aspects of development, hosting, system upgrades, security and maintenance.

Architecture

Skillport uses a three-tier application architecture with an interface layer, business logic layer and data layer. The interface layer provides both web-based and web-services based interfaces to the application. Skillport features a rich AJAX presentation layer that presents an engaging, interactive experience to learners and admins. While OLSA (Open Learning Services Architecture) forms the basis of a Service Oriented Architecture (SOA) that simplifies integrations between Skillport and third party systems.

The business logic layer provides primary logic controls to the application. The logic is divided into sub-systems representing major functional areas of the application using an extensible object-oriented server side Java framework. The data layer utilizes a relational database to provides data persistent services for both primary application data and client-specific data. Each customer has a dedicated database instance ensuring complete segregation of client data. Both data and application tiers are load balanced across multiple servers for optimal performance.

Skillport's application architecture allows clients to enjoy an turn-key deployment, worry-free maintenance and frequent enhancements of a SaaS solution with the security of a private client database.

Authorization and authentication

Skillport uses a Role-Based-Access-Control (RBAS) security model with an account-based authentication model. User accounts are created and granted specific privileges to various system capabilities and access to all or some of the client data. Users are required to provide a username and password combination which is associated with their user account. These credentials are stored and maintained within the Skillport application. The system provides robust security options including custom password composition rules, password management and recovery options and account lockout options.

In addition, Skillport supports single sign-on (SSO) utilizing:

- SAML 2.0
- Skillsoft-proprietary SSO
- Custom SSO

Use of SSO provides for a better user experience and enables organizations to utilize existing authentication systems and processes. Skillport can support both Identify-Provider initiated and Service-Provider initiated SAML processes.

Integration

The Skillport interface layer is extended through a set of turn-key services as well as custom capabilities to support the integration of the LMS into existing client infrastructure. This includes integration with HRIS, directory services, portals, CRM, e-commerce, business intelligence and other systems to create a solution capable of leveraging existing client processes and data.

These services include both a SOAP-based web service API (OLSA) and a proprietary API (BCS). Documentation for these APIs can be found by visiting: http://documentation.skillsoft.com/ikb/

Skillport has standard data import and export services built into the application. Standard import tools are provided for learner data, organizational/group data and course content. Exports are available in HTML, CSV, PDF and Excel from the Skillport reporting system.

In addition to the standard import/export tools, Skillsoft can support custom data exchange solutions. These enable clients to establish custom processes for moving data to and from their existing systems. Please contact your account executive or application engineer for more details regarding custom data services.

Non-Skillsoft learning management systems

Skillsoft's SOAP-based, Open Learning Services Architecture (OLSA) API is utilized by leading LMS vendors to enable the rapid deployment of Skillsoft learning assets on those systems. This solution enables learners to access Skillsoft training directly from their non-Skillsoft LMS. It also simplifies the deployment of Skillsoft content for LMS administrators. For more information on OLSA visit: http://documentation.skillsoft.com/ikb/

Unless otherwise noted, all technical details in this document pertain to Skillport whether accessed directly or via a non-Skillsoft LMS.

Configuration and customization

The Skillport application is designed to be highly configurable. Most changes to configuration can be managed through the administration site and include:

- Security settings
- Course completion rules
- Catalog behavior
- Branding
- Communications
- Other general site preferences

Security

Skillsoft takes the security of its customer's data very seriously. Our policies, procedures and applications are all designed to ensure the safe management of client data. Skillport is designed to manage as much or as little organizational and personal data as your organization is comfortable sharing. Typically data exposure includes

- Names
- Email addresses
- Employee IDs
- Organizational structure
- Training results

The following is Skillsoft's security policy which is the foundation by which all Skillsoft security processes and procedures are developed and maintained.

SKILLSOFT SECURITY POLICY

It is the policy of Skillsoft to protect its information assets in accordance with all applicable federal and state statutes and regulations, as well as with effective information security practices and principles generally accepted as 'due diligence' within the learning solutions business community.

The Company specifically prohibits unauthorized access to, tampering with, deliberately introducing inaccuracies to, or causing loss of Skillsoft's information assets. It also prohibits using information assets to violate any law, commit an intentional breach of confidentiality or privacy, compromise the performance of systems, damage software, physical devices or networks, or otherwise sabotage Company information assets.

Skillsoft protects its information assets from threats and exploits, whether internal or external, deliberate or accidental. The degree of protection is based on the nature of the resource and its intended use. The Company recognizes that no single office, policy, or procedure provides absolute security; therefore, all Company employees and other stakeholders share responsibility to minimize risks and to secure the information assets within their control.

The Company shall take appropriate action in response to misuse of Company information assets. Any violation of this policy may result in legal action and/or Company disciplinary action under applicable Company and administrative policies and procedures. Distribution of specific procedures implementing this policy includes, but is not limited to, web pages, email and printed documentation.

Infrastructure security

Network security

Skillsoft uses a multi-tiered perimeter defense infrastructure ensuring the greatest possible protection from unauthorized access or malicious activities. Measures include a most-restrictive firewall policy, network and pattern-matching intrusion detection and prevention systems as well as an extensive and current anti-virus infrastructure. See ***Infrastructure components*** for additional details.

System configuration

All systems are constructed from standardized, pre-hardened images using industry best practices in accordance with Skillsoft specific system and software requirements. Routine and ongoing patch management is controlled via centralized patch management software ensuring a consistent and current posture.

All operating systems are loaded with the most current updates from the OEM. This is done using a suite of externally and internally developed tools. All systems are hardened to limit unauthorized Admin or Super User access using industry and vendor best practices including:

- Complex naming and password standards
- User access control settings
- Redirection to disabled accounts

All systems are checked to ensure that any unnecessary or potentially exploitable services are set to be disabled at power on.

Access policy

System and Facility access control is governed by a select body of Skillsoft Hosting Services personnel. System access is granted at a level commensurate with job function. Access to security and network devices is restricted to the Network Management team, the Hosting Manager and the Senior Hosting Analyst. Hosting Facility access is managed in conjunction with the collocation service provider through a formal ACL. Governance of this ACL is restricted to Hosting Managers.

Access to all Hosted Systems is restricted to Skillsoft Hosting Services personnel. In select cases Vendor-authorized technicians are afforded access to the systems in conjunction with hardware failure events or professional services engagements.

Remote access to the hosted environment

All privileged access and communication to the Hosting environment is secured through either client or site-to-site encryption. Site-to-site tunnels providing privileged port or service access are restricted to Skillsoft Hosting-Only subnets. Remote access authentication is tightly integrated with existing domain security and provides for a single point of administration. Remote access is restricted to Hosting personnel. This policy is universal and comprehensive to include administration, backups, etc. Under no circumstances is privileged access afforded to developers, Account Consultants, corporate IT or Account Executives.

The production system can be accessed only by the Hosting Engineers. Access to the various subsystems is segregated based on duties and responsibilities. Since most hosting engineers need access to the hosting environment 24/7, they have laptops—however the laptops have only the operating system and VPN software on it. To access the hosting environment the hosting engineers connect remotely from their laptop to their desktop machine on Skillsoft premises, which has the VPN software that provides connectivity to the Hosting environment. The access is authenticated via a two-factor authentication from RSA Security. Application passwords are changed every 30 days or when an individual in hosting leaves their job role.

Physical security

All Skillsoft hosted systems are located in a third-party SSAE 16 Type II compliant facility providing 24x7 access control to a defined access control roster. The facility employs multilayered access control governances including mantrap doors, CCT, card-only access and 24x7 guards. Premises are unmarked. See ***Infrastructure data center*** for additional details.

Data protection

Skillsoft's data protection practices include the following:

Data retention and protection

Data storage – All customer data is stored on an enterprise storage array providing the maximum degree of data protect and integrity available. Customer data is stored exclusively in relational databases with no data present on Internet-facing web systems. Access to this data is restricted to Hosting personnel and only duplicated to tape format. Tapes are encrypted following the FIPS 140-2 standard required by DoD and Federal. In some cases customer data is duplicated into a secured and controlled lab environment for the purposes of issue resolution or capacity planning exercises directly relating to the customer. Customer data used for this process goes through a "scrubbing" process where all customer Personal Identifiable Information (PII) is removed. Customer data is stored in a dedicated database schema for each customer.

Data protection – Access to database systems and customer databases is restricted to Hosting personnel only. Privileged remote access is exclusively conducted over a secure, encrypted channel. Off-site tape backups are entrusted to a leading authority in data and tape storage with the media stored at a remote, secured facility and accessible only to a restricted group within the Hosting Services organization.

Data encryption – Customers' user account passwords are encrypted in their respective database using a SHA 256 hashing algorithm.

End-user access methods – All data access occurs through the application via HTTPS. Direct access to the database is never afforded.

Data availability following contract termination – If requested as per the terms of the original Master Service Agreement, Skillsoft can make available to the customer all progress and user data delivered to the customer in a mutually agreeable file format.

Third party annual penetration test - In a continuing effort to improve the security of the Hosted environment, Skillsoft contracts a third-party security organization to conduct an annual full penetration and vulnerability assessment of the hosting environment. This assessment reviews firewall policies, intrusion detection and prevention policies, system patch levels, vulnerability to known software exploits and brute force attacks. Additionally Skillsoft conducts internal penetration tests on an on-going basis.

TRUSTe – Skillport.com application is TRUSTe and Safe Harbor Certified. For more information visit: http://clicktoverify.truste.com/pvr.php?page=validate&url=www.skillsoft.com&sealid=102

Skillsoft policies

Skillsoft's security policies include the following:

Security breach management – In the event that Hosted systems or services are compromised, Skillsoft Hosting Services will immediately implement an environment lock-down blocking all inbound and outbound communication from the datacenter environment. Privileged remote connectivity would be maintained for Hosting Security and Network personnel to ensure the timeliest resolution of the issue. Every effort would be taken to close the breach, re-stabilize the systems and limit exposure of customer data. A detailed post-mortem of the events would be conducted at the earliest opportunity and shared with our customers as appropriate.

Process for communicating back to customers – Communications to the customer are effected through Skillsoft Learning Consultants with root cause analyses available to customers upon request.

Vendor, technology and platform disclosure – As a security countermeasure, Skillsoft will not release to customers the make, model or manufacturer of any network or security device in use within the Hosting facility. This includes, but is not limited to, the release of information regarding:

- Firewall related hardware/software/settings
- Intrusion detection system related hardware/software/settings
- Network penetration testing
- Vulnerability scanning
- Network topology
- Internal IP scheme
- Operating systems configuration and security settings
- Software vendors and version used

Report to customers regarding a security violation incident – If a security incident occurs, information related to the incident will be provided via Skillsoft's Tech Support team to the customer's primary contact. The first phase of the contact will acknowledge that a problem occurred and the status of the remediation. Subsequent updates will be sent during the

remediation process. Once the incident is closed, Hosting will conduct a root cause analysis and the results will be provided to customers upon the customers' request.

System documentation – Extensive documentation has been created covering all aspects of system construction, application installation and product configuration and management. These documents are constantly updated to reflect the most current policies and procedures. All documents remain under strict version control and any changes are subject to multi-party reviewed and approved.

Skillsoft staff

Skillsoft's staffing policies include the following:

Roles and responsibilities – Skillsoft has assembled a world-class team of IT professionals with an organizational structure that provides clear lines of accountability, oversight and ownership without sacrificing agility and responsiveness to customers.

Skillsoft recognizes the unique challenges facing service providers and the specialized skill sets required to effectively manage and grow Hosting infrastructures. In direct response to this, Skillsoft has heavily invested in a dedicated Hosting Services team whose sole mandate is to ensure the best possible experience for our Hosted customers. The Hosting Services team is generally divided into the following teams:

- Networking and Security
- System Analysts
- Application and Systems Administrators
- Database and SANS Administrators
- Product Support and Fulfillment
- Program Management

Employee background checks – Skillsoft recognizes the sensitivity of the data handled by the Hosting employees. To ensure the best security awareness and due diligence, Skillsoft performs background checks (subject to applicable local laws) with respect to pre-determined positions that require access to customer data. Skillsoft also checks references provided by candidates generally as part of the application process. Additionally all Hosting employees are required to review and sign a Security and Privacy policy that details roles and responsibilities, escalation procedures and overall code of conduct with the Hosting organizations. All Hosting employees are required to sign the policy acknowledging their understanding and commitment to its guidelines.

Dedicated hosting team

Personnel training – In an ever changing and evolving technology landscape, Skillsoft recognizes the critical role training plays in the successful delivery of services. To ensure that Skillsoft has the best possible resources available to its customers, Skillsoft aggressively pursues training for all products resident in the Hosting Infrastructure. This includes a formal training agenda for proprietary products developed by Skillsoft.

Password management – Skillsoft Hosting Services password policies include:

- All passwords expire every 30 days
- Minimum length and complexity requirements
- The use of mixed case
- The use of alphabetic and non-alphabetic characters

Efforts are made to limit the communication of passwords to verbal channels and passwords are provided on a need-to-know basis. When verbal communication of passwords is not possible, username and password combinations are communicated in separate correspondences and only to the target audience. Sharing of user account passwords is strictly prohibited.

Personnel changes – Employee actions (hiring, terminations, suspensions, etc.) are fully coordinated with Human Resources and corporate IT providing immediate and coordinated responses to all Hosting personnel status changes. Additionally, Hosting management is apprised of all Skillsoft staff terminations should special measures be required to protect against actions of ex-employees with privileged knowledge or understanding of Skillsoft proprietary software.

Data Encryption and external storage – Skillsoft utilizes file-level encryption strategy leveraging software that seamlessly encrypts files at rest and in transit based on risk-levels, as defined in the information policy. The risk-factor is determined as a combination of content, context and type of data. All customer data is defined as sensitive information and treated accordingly. For data that can potentially be copied to external storage devices such as USB thumb drives, CD and DVD, an Enterprise Information Protection software will detect and prevent Skillsoft's employees from transferring customer information.

Wireless access – Skillsoft provides to its employees wireless access within Skillsoft facilities. The wireless service uses WPA2 Enterprise encryption for access to Skillsoft network environments. All wireless access requires unique authentication and is logged to a central location which is reviewed for failed access attempts. Rogue wireless detection is performed continuously to prevent malicious activity.

Wireless access is segregated via its own Ethernet interface on Skillsoft's Firewall with no access to internal corporate resources. VPN must be utilized to gain access to corporate resources.

Infrastructure

Data center and co-location services

Skillsoft contracts data center and co-location services with Tier 1 service provider, SunGard. The location of the data center is within 60 minutes of Skillsoft's Nashua office providing close physical access should it be necessary. SunGard data centers provide redundant high-bandwidth connectivity and scalability enabling Skillsoft to develop its hosting service rapidly and effectively.

Security includes multiple levels of physical and digital access controls. SunGard delivers highly reliable network connectivity and state-of-the-art collocation facilities providing the best possible operating environment to Skillsoft and its customers.

The SunGard data center includes:

- VESDA fire detection and FM-200 fire suppression.
- A 2N redundant power supply provides dual power feeds and backup batteries, water coolant systems and generators.
- An N + 1 redundant climate control system provides primary and backup chiller units, cooling towers and water storage.
- A local network operations center (NOC) monitors the data center's operations continuously with 24x7 guards with interior and exterior closed-circuit television surveillance.
- Electronic access at all data center entrances, including electronic key management systems and individually keyed cabinets and cages.

Additional information about SunGard data centers and co-location services can be obtained from SunGard directly.

Infrastructure components

Skillsoft has made strategic investments in best-of-breed devices from industry-leading vendors, reflecting our ongoing commitment to deliver world-class service. The items below outline the key components and characteristics of the infrastructure supporting the Skillport application. Skillsoft does not share detailed specifications, vendor, model or version information of infrastructure components or tools.

Firewalls

Skillsoft has selected best-of-breed hardware and software solutions from established industry leaders. Firewalls utilize a most-restrictive policy providing only for known and require port access. Access to firewalling systems is strictly controlled and adjustments to any firewall policies are subject to managerial approval prior to implementation.

Intrusion detection prevention (IDP)

Through granular pattern matching and event correlation Skillsoft provides comprehensive protection against known vulnerabilities and zero-day defense against emergent threats. IDP signatures are considered and updated on a continuous basis.

Intrusion detection system (IDS)

A redundant, active IDS implementation provides effective and proven protection against brute force and denial of service attacks. Adjustments to the IDS configuration are considered on a continuous basis.

Load balancers

Inbound traffic is managed by redundant front-end network-based load balancers. Requests are

distributed across multiple server farms to ensure optimal performance and a consistent end user experience. Network Load Balancing provides scalability and high availability to enterprise-wide services.

Three-tier architecture

The application architecture utilizes redundant, front-end web servers. The application runs on a load balanced middle tier. Each server is a multi-processor, multi-core system connected via fiber to database servers managed on an enterprise storage device.

Database servers

Production database servers are configured in an n+1 configuration. Each server is a multi-processor, multi-core system connected via fiber to enterprise database storage.

NAS/SAN

Enterprise class mass storage systems are utilized for courseware storage and various content files. Redundant connections to these devices exist for all attached servers. The infrastructure servers at a rate 250 – 300 mbs.

Local area network

All components of the Local Area Network are fully redundant. A distributed network topology is utilized with high bandwidth layer 3 switches at its core. All servers are connected via redundant gig uplinks.

Secure data transmission

When elected by a client, all client-server communications and data exchange is protected by 128 bit encryption provided by a recognized Certificate Authority. In certain scenarios customers elect to provide user data directly to Skillsoft for direct insertion into Skillsoft Hosted applications. Skillsoft provides the option of a SecureFTP transfer if this service is requested.

Redundancy and scalability

Skillsoft applications and their supporting infrastructure are designed and deployed, from inception, as a Software-as-a-Services (SaaS) solution. Availability and performance are key requirements for every SaaS implementation and infrastructure redundancy and scalability are fundamental in achieving these requirements.

Capacity management

Skillsoft capacity planning ensures application availability very for new products, new customers, customers' upgrades and systems replacement.

The Skillport application and its add-ons are deployed based on a pre-defined deployment plan that maps out exactly how many Skillport applications will share the same hardware pool and how will the hardware pool be configured. The required hardware is pre-built and configured based on build sheets and pre-configured images that were created by the system analysts. The existing hosted

environment is continuously monitored for resource utilization. Since emergency situations may arise, the hosting department has 'standby' inventory ready to be deployed to address any capacity issues that may arise. All Skillport versions are subject to load testing to validate the hardware requirements and the deployment configuration.

Load balancing

All current generation products achieve maximum scalability and service availability through a classic hardware load-balanced architecture. All real-time application level components provide both horizontal and vertical scalability options and are constantly monitored against key performance criteria and are appropriately scaled on demand. Core infrastructure components are implemented in either an active-active, or active-passive failover model.

Hardware failure

Many systems in the Hosting Environment are hardware load balanced and the loss of a system is not service affecting. In cases where hardware redundancy is not provided, fully configured, hot-standby systems are available for immediate use. Recovery policies and procedures are documented to enable quick response to such incidents.

Application malfunction

Application faults are detected through continuous system monitoring and mean time to resolution in generally less than 10 minutes. Procedures for corrective actions are documented and all application faults are escalated to development for investigation.

Network loss

A fully redundant network infrastructure enables Skillsoft to provide the most highly available infrastructure possible. Redundancy is provided at all levels including the Internet connection. Failover tests are conducted on a regular basis to ensure that configuration modifications and patch installations did not affect the reliability of our fault tolerance.

Trusted recovery

In the event that a third party needs to be involved in a system recovery, the third-party engagement will be subject to formal contract terms which are reviewed and refined by the Skillsoft legal team before engagement. Third-parties directly handling sensitive information are subject to and bound by Non-Disclosure Agreements.

Akamai

Skillsoft uses Akamai to improve content delivery performance in the EMEA and APAC regions. The Akami service is used to expedite the course delivery to the end user. The application and the student progress tracking are done by Skillsoft within the Skillsoft hosting environment.

Disaster recovery

Skillsoft's disaster recovery policies include the following:

Disaster recovery (DR)

To facilitate the most rapid recovery possible, Skillsoft Hosting Services has a documented disaster recovery plan that details the responsible parties, the communication protocol and the steps that will be taken in the event of a disaster. Skillsoft has a redundant hosting site located in Aurora, Colorado. The redundant site is at a distance of, 1900 miles from the primary hosting site, located in Boston, Massachusetts. Both sites are managed by SunGard Hosting Services. The two facilities are setup in an active-active configuration, with a target RPO of 180 minutes and a target RTO of 12 hours.

The primary and the DR sites are linked via a dedicated 10GB line replicating customer data between the two sites on a continuous basis. The replication uses a disk block-based replication technology. Additionally, disk-based backup devices in Boston are continuously replicated to a redundant device in Aurora. Skillport applications are configured to use a native, vendor-supplied virtual machine recovery suite which provides rapid and fully automated recovery of the infrastructure to the remote facility.

Skillsoft conducts an annual DR test staging a failover of a sample of its SaaS infrastructure. Testing results are available to customers upon request

Overall backup strategy

Skillsoft Hosting Services has invested in a multifaceted backup strategy that blends the best features of traditional tape, block-based disk copies and secondary disk storage.

Backup schedule for application data

In order to ensure the greatest possible flexibility and speed-of-recovery minimal data is stored on application servers. Application data is stored off-site on an independent disk infrastructure which is accessible to the Hosting Infrastructure with minimal latency. In cases where primary data exists on application systems, this data is relocated to a central disk repository and committed to tape each night.

Backup schedule for client data

Database data files are backed up using two separate but complimentary methods. The first is a block-based disk copy to a set of independent disk on the storage array which enables Hosting Services to conduct complete data file backups of all databases every three hours. Because of the light-weight and fast nature of this operation it can also be done ad-hoc in advance of scheduled maintenance activities to ensure point-in-time recovery to a pre-maintenance state. Additionally, data is committed to tape each night.

Log files

All pertinent log files are automatically relocated to a centralized disk library each night and retained there indefinitely. They are additionally committed to tape on a nightly basis.

Backup encryption

All SQL backups utilize FIPS 140-2 compliant software encryption using 256-bit AES encryption with randomly generated 64 character pass phrase.

File backups

- Network Attached Storage (NAS) - NAS data is committed to tape via NDMP backups with customized full and differential backup schedules. NAS data includes all course and Dialogue content as well as various customer-specific assets such as logos and graphics.
- Product and customer specific files are backed up with a customized differential and full back up schedule.

Backup rotation

- Tapes are collected from the Data Center every Wednesday and secured in a third-party off-site facility; tapes are moved back into rotation once data has expired.
- Skillport Database daily full backups are retained onsite for 3 months in disk based storage unit.
- Skillport Database weekly full backups are retained onsite for 6 months in a disk-based storage unit and LTO tape media are retained for 1 month at an offsite 3rd party storage facility.
- Skillport Database monthly full LTO tape media backups are kept at an offsite 3rd party storage facility for 36 months.
- Skillport Database yearly LTO tape media backups are kept at an offsite 3rd party storage facility for 60 months.
- Administrative server differential backups are stored on disk-based storage unit for 3 months and monthly full backups to LTO tape media are stored at an offsite 3rd party storage facility for 36 months.
- Product and customer specific backups are retained onsite in the disk-based storage unit per Hosting data retention requirements defined in internal documentation. Monthly full backups to LTO tape media are retained at an offsite 3rd party storage facility. Product and customer specific data on LTO tape media is set to never expire.

NAS backups are retained onsite in the disk-based storage unit per Hosting defined data retention requirements defined in internal documentation.

Offsite storage

Skillsoft uses Iron Mountain for its offsite backup storage. Iron Mountain is responsible for the secure transport and storage of the backup media.This partnership is governed by an aggressive SLA that ensures that Skillsoft Hosting Services is able to restore services to customers at the earliest opportunity and minimize any service disruptions.

Recovery time from backup

Depending on the nature of the fault and the historical requirements of the data recovery times will

vary. Recovery of data from a block-based disk backup and full restoration of service is expected to be complete within 60 minutes of initiation. Recovery and restore of historical data from a remote facility including full service restoration is expected to complete within 8 hours.

Monitoring and virus protection

Monitoring of the application, infrastructure and Internet connectivity is critical to ensuring availability and performance commitments are achieved. Skillsoft uses a variety of tools deployed both internally and externally to ensure this is effectively accomplished.

Restart and recovery procedures

A comprehensive monitoring infrastructure ensures that Skillsoft Hosting personnel are alerted at the earliest opportunity of service affecting conditions. Clearly articulated governances inform the assigned Hosting Engineer what actions are permitted without escalation and specific details on how prescribed actions should be undertaken. In the event that a condition arises for which there is no defined procedure, the issue is escalated to a manger for resolution.

Outages management

All Hosted Systems are broadly monitored for availability from multiple physical locations. Visual and auditory alerts are generated within 1 minute of a service fault and email alerts generated within 2 minutes. Immediate action is undertaken to restore impaired services. All service affecting events are logged and analyzed by both Development and Hosting resources to ensure that the event is fully understood and steps are taken to mitigate future exposure to the event.

Slowness in applications performance

In addition to tracking the availability of Hosted services, comprehensive measures are in place to protect against subtle or transient application latency. A redundant and geographically dispersed monitoring infrastructure provides visual, auditory and email notification for any monitoring event that surpasses the allowable time limit. The transactional monitors emulate user activity and provide a reliable indicator of general end-user system performance.

Impaired application performance (i.e. latency)

Application latency is detected through continuous system monitoring and mean time to resolution is generally less than 10 minutes. Procedures for corrective actions are documented and all application latency events are escalated to development for investigation.

System logs

Logs for a wide range of application and infrastructure activities are generated including:

- System logging captures all events relating to system access including privileged user right use, service stops/starts and sys admin logins/logouts.
- Firewall and network intelligence logs capture all failed access events and suspicious activities as defined by our IDP/IDS infrastructure.
- Comprehensive syslog and SANS/Storage management logging capture all non-standard events.
- Detailed application logs trap all unusual application events in addition to verbose web server logs.

All system, security and access logs are retained by Skillsoft Hosting services for an indefinite period. All event logs are archived daily to centralized disk storage for convenient access. This centralized repository is then committed to tape and retained according to our tape retention policies as defined in this document. Access to logs is restricted to Hosting personnel with the exception of application error and web logs which are shared with Skillsoft Development on an as-needed basis.

Virus protection

Skillsoft virus policies include the following:

Virus protection

System level virus protection and prevention is afforded by a centralized virus management system. This centralized system facilitates a rapid response to emergent threats and ensures a uniform posture across all hosted systems.

Vendors that work on the premises with their own laptops are subject to virus scan and virus update by Skillsoft's IT department prior to connecting to Skillsoft's network.

Frequency of signature updates

Virus signature updates are reviewed and deployed on a continuous basis in response to emergent threats. Hosting maintains a very tight schedule for antivirus updates maintaining the both the application and the virus signatures up-to-date.

Release management

Skillsoft's release management process has been designed to seamlessly support a steady stream of application enhancements along with third-party product updates and infrastructure upgrades and patches. To support this process, guidelines have been established for each type of release (application, infrastructure, etc.), which govern the cadence by which changes are introduced.

Application

Product development – Product related software development is done by Skillsoft Engineering staff, which consists of System Architects, Application Engineers and Database developers. The engineering department is divided by the various areas of expertise required by the various products and their respective development life cycle.

QA processes – A dedicated Quality Control team ensures all software made available to customers is of the highest quality and performance. This team has final veto authority for all software packages moving to production systems.

Qualification processes – An extensive and comprehensive testing matrix is applied to all Skillport software releases testing functionality and support for a wide variety operating systems and browser versions. New functionality is tested extensively and existing functionality is additionally tested to safeguard against regressions.

Software rollout into production – Following a formal release to Skillsoft Hosting Services the software release package is reviewed by Hosting Services and a deployment strategy is assessed.

Software then enters a controlled release cycle—initially deployed to a small, pre-determined number of systems. Following this controlled release, a general release cycle is undertaken with all systems receiving the update over a series of scheduled maintenance windows.

Patch management and version management – Continuous improvements to software occasionally result in patches being available to Skillsoft software product lines. All major and minor software releases including patches are uniquely versioned and this version in transparent to all operators. The release strategy for Patch deployments models that of the general software release process described above.

Software development

Software development process – Following the finalization of functional specifications, general software architecture is determined by the product software Architect and a Hosting Services Architect. In some cases Architectural considerations may result in changes to functional specifications. These adjustments are communicated back to the respective stakeholders and a final functional specification and Architecture is determined. This architecture is documented and released to the development manager for review, project scoping and resource assignment.

Access to source code – All software access and versioning is strictly controlled through a software source control package. Access to source code is provided on an as-needed basis and is exclusively restricted to Skillsoft Software Engineering.

Software release process – Authority to release software from development to QA is restricted to the development manager responsible for the product line. Authority to release software from QA systems to final qualification systems is restricted to the assigned Quality Control Engineer provided the software has met the pre-defined acceptance criteria for release. Authority to release software from final qualification to Skillsoft Hosting Services is restricted to the assigned Quality Control Engineer (with QA Manager assent) provided the software has met the pre-defined acceptance criteria for general release.

Infrastructure

System configuration - management – Adjustments to system images or configurations are strictly controlled through a multi-party review and approval process involving Management, Network and Security, System Analysts Architects and System Engineering resources. Documentation is immediately adjusted in response to system reconfiguration.

Change process, testing and approval process – Change requests are submitted by the initiating party to the appropriate technology manager for initial consideration. The area manager will then invoke guidance of the Hosting Manager to determine the scope of the change and establish an approval roster. Whenever possible changes are vetted through advanced implementation in a staging environment and in some cases warrant and receive load testing by a dedicated automation team.

To ensure the quality of work, changes to the environment are verified by Hosting Supervisors on an ongoing basis. The Hosting Analysts conduct physical audits quarterly to ensure that the environment meets the defined standards.

Configuration and security specification – Skillsoft employs a "most-restrictive" policy in regards to all network device policies and access controls. Firewall, IDP and IDS rules are continually reviewed and monitored for suspicious events. Device configuration is standardized and heavily documented. Adjustments to configurations and policies are reflected in the associated system or device documentation.

Configuration control – Adjustments to any device by a network technician require the approval of the Network Manager and in some cases will additionally require the Hosting Manager's approval. An adjustment to any aspect of host system configuration requires the review and approval of the Senior System Analyst and in some cases the Hosting Manager. All configuration adjustments or changes are reflected in the associated system or device documentation.

System maintenance – Description of planned system maintenance schedule
Skillsoft currently provides for 2 weekly routine maintenance windows. They are as follows;

- Wednesday: 1– 2 a.m. EDT/EST
- Sunday: 1 – 3 p.m. EDT/EST

Activities conducted in these maintenance windows may include, but is not restricted to, hardware maintenance and replacement, system patching, infrastructure enhancements and Skillsoft software releases.

Customers located in the Asia Pacific region, have the option to elect for an alternate Wednesday maintenance window.

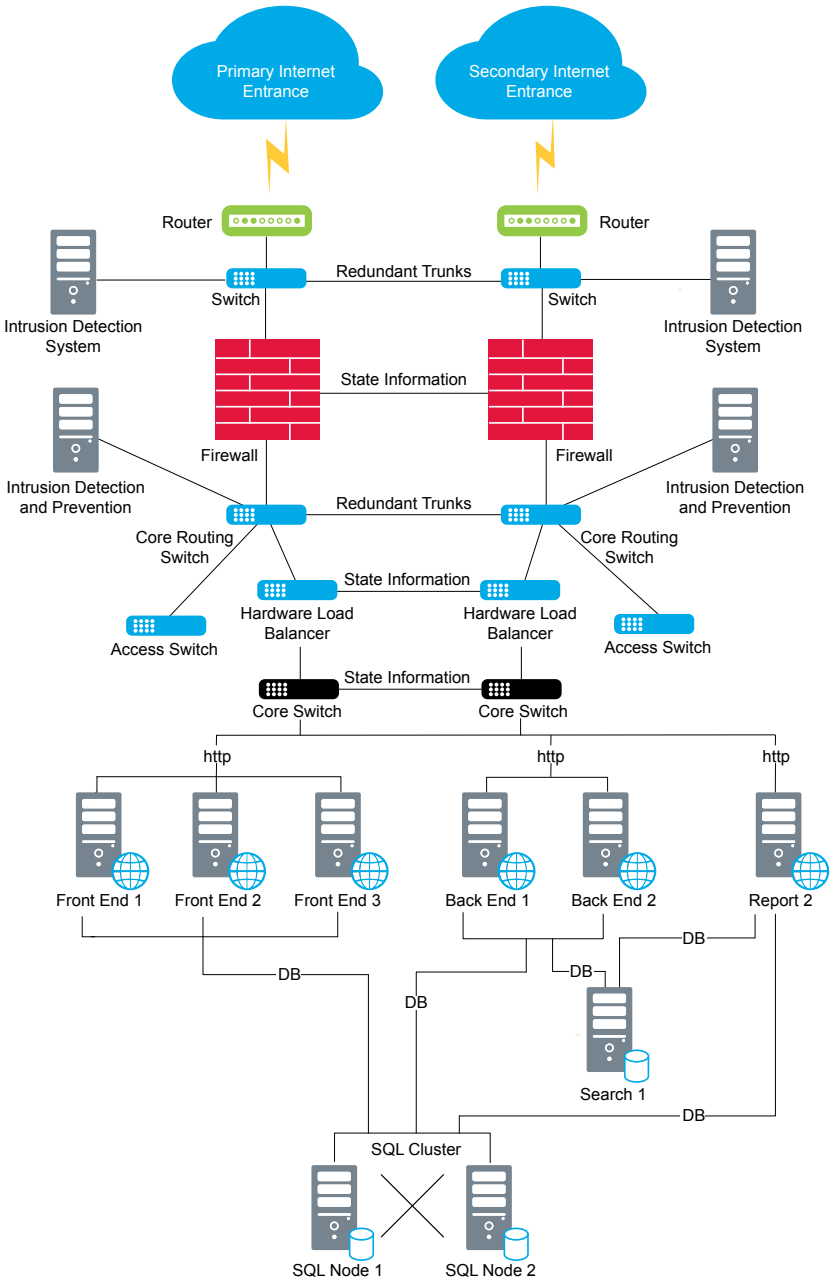
Emergency maintenance – Skillsoft reserves the right to conduct unplanned maintenance activities when a delay of said maintenance is seen to pose a significant risk to the availability and or security of the services provided. Every effort is made to coordinate these unscheduled maintenance activities with clients in advance and to conduct these activities at the least impactful time as circumstances allow for.

Maintenance schedule – All scheduled maintenance window activities are coordinated and planned in advance with established cut-off windows. All activities are critically examined to ensure timing and that all activities are non-overlapping.

Software – A centralized patch management software suite ensures a consistent security posture across all managed systems and empowers Skillsoft Hosting services to aggressively respond to emergent threats. All available software patches are considered by Hosting Analysts and deployed on a schedule in accordance with the associated risk.

Security and network devices – A dedicated team of network and security professionals continuously consider newly available patches and enhancements to network and security devices. Signature bundles for IDP and IDS devices are downloaded daily and considered for implementation on a continuous basis.

Appendix 1 – Skillsoft customer-facing topology



For more information or to learn more,
call 800-327-6960 or visit www.skillsoft.com