



Protecting Your Data: Secure, Stable Project Collaboration from Autodesk

Autodesk® Buzzsaw™ and Autodesk Streamline™ are web-based project collaboration services for the building and manufacturing industries, respectively. This document shows how Autodesk's high level of professional service meets the needs of building and manufacturing users.

This document covers the following topics:

- Technology and environments
- Security
- Monitoring and operational practices
- Disaster recovery

Autodesk strives to deliver the best service possible. To achieve this, the first goal is to provide a solid systems framework. We continually perform architectural reviews to ensure that all systems are performing optimally. Layering applications on top of the stable Autodesk® ProjectPoint™ platform allows us to support additional industry-specific applications without significant changes to operational practices.

This layering approach can be seen in our systems infrastructure, security, monitoring, and operational practices.

Technology and Environments

The infrastructure for the Autodesk Buzzsaw and Autodesk Streamline environments is

- Fully fault tolerant with no single point of failure
- Adaptable to increasing demand with no impact on performance
- Stable because it is based on industry best practices

These principles apply to all aspects of Autodesk Buzzsaw and Autodesk Streamline infrastructure; for example, these services implement

- Mirroring of all network components such as firewalls, routers, load balancers, switches
- Load balancing of traffic over multiple web servers
- Instantaneous routing to backup servers if problems occur
- Multiple CPUs, power supplies, network connections, fan units, and so on for all servers

In addition to duplicating components at all levels, Autodesk works with recognized leaders in hardware and software systems:

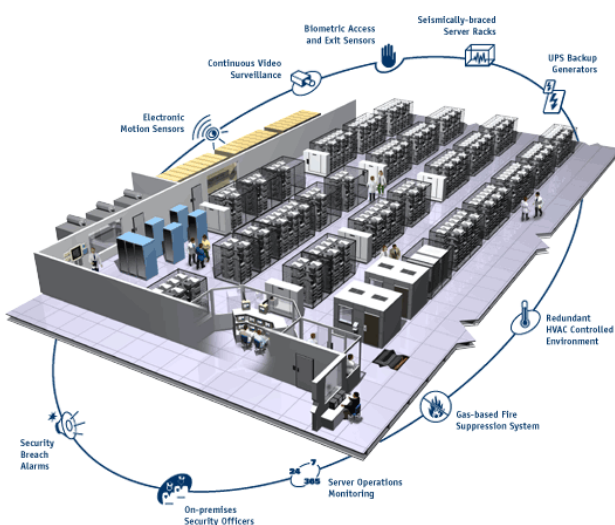
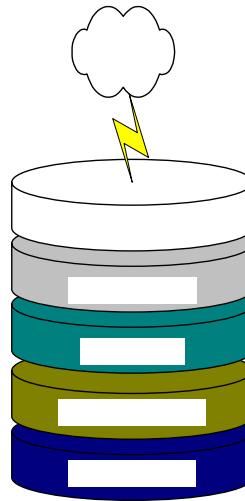
Protecting Your Data: Secure, Stable Project Collaboration from Autodesk

- Microsoft: Microsoft® Windows® 2000, SQL 2000 database, Internet Information Service
- HP (Compaq): ProLiant® Intel® Server series
- Cisco: Firewalls, routers, switches, and other network equipment
- Nortel: Alteon™ load balancers
- EMC: SAN and NAS data storage systems, data replication, and backup systems

Security

Autodesk has developed a multilayer approach to security, using the following technologies and configurations:

- All data passed between the user's client and Autodesk systems is encrypted with Secure Sockets Layer (SSL) technology. Verisign registered certificates provide the encryption keys.
- Firewalls strictly control access to Autodesk servers from the Internet as well as Autodesk's internal corporate networks.
- Within the data center infrastructure data flow, strictly defined rules ensure that only authorized communication occurs between systems.
- All servers are required to be at a defined level of security lockdown. This includes closing all unused layer 4 ports and ensuring that all servers have the latest security patches installed.
- Only application system accounts and Operation Team member accounts exist.



Physical Access and Security

Cable & Wireless (Exodus) supplies our primary data center and provides security for our systems, including

- Access list updated only by Autodesk's Operations Managers. Not even our own Operations Team has permanent access.
- Surveillance monitoring of facility.
- Onsite security presence.
- Biometric access and exit scans.
- Fire suppression systems.
- Redundant backup power generation.

Administrative and Remote Access

Access to administer systems is controlled by the following:

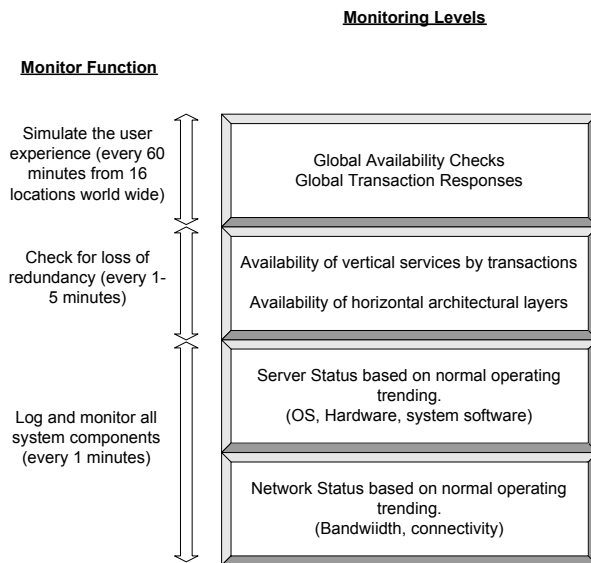
- Only Autodesk Operations Team members have Administrator accounts. Activity is monitored and audited through firewall and system logs.
- Administrators can log in only from workstations with specific network IP addresses in the Autodesk office.
- When team members are remote (after normal hours) they can connect to the systems only through a dedicated VPN 3DES connection using a RSA SecurID token.

To ensure that Autodesk maintains this high level of security and to improve security in the future, we perform regular audits by

- Checking security logs for unusual activity
- Scanning all equipment for known security holes
- Checking patch levels on all equipment and software

Monitoring and Operational Practices

Providing high levels of availability requires a comprehensive set of system monitors and operational practices. The aim is to predict problems and correct them before users are impacted or service is interrupted.



Autodesk performs all the standard checks normally associated with systems:

- Processor
- Memory
- Disk space
- Network traffic
- Software service active/inactive
- Interface status

This monitoring is carried out on

- Network equipment
- Server hardware
- Server software
- Storage systems

Based on normal system operating parameters, Autodesk follows a defined escalation procedure for any element outside acceptable limits. Taking corrective action within 15 minutes, combined with the redundant architecture, ensures that users are not affected.

Autodesk then analyzes this data to plot historical trends for capacity planning and problem resolution. This information helps predict the need to increase processing power on any tier of the architecture, increase bandwidth, allocate additional storage, and so on.

Protecting Your Data: Secure, Stable Project Collaboration from Autodesk

	Total 22.62 sec (DNS 0.00 sec, connect 0.75 sec, response 17.84 sec, download 4.03 sec), no frames, 22 images (48K total)	www.buzzsaw.com Http-Get Monitor	Tools Edit Refresh	11:26 AM 7/31/01	X
	30.70 sec, 4 steps, 25K total, no frames, 10 images	URI Transaction: http://project-ost.buzzsaw.com/warehouse	Tools Edit Refresh	11:24 AM 7/31/01	X
	38.85 sec, 4 steps, 68K total, no frames, 10 images	URI Transaction: http://project-ost.buzzsaw.com/buzzsaw	Tools Edit Refresh	11:26 AM 7/31/01	X
	7.65 sec, no frames, 3 images (22K total)	URI: http://64.75.26.26/client/buzzsaw	Tools Edit Refresh	11:26 AM 7/31/01	X
	1.53 sec, no frames, no images (203 bytes total)	URI: http://plansandspecs.buzzsaw.com	Tools Edit Refresh	11:26 AM 7/31/01	X
	31.76 sec, 4 steps, 25K total, no frames, 10 images	URI Transaction: http://myfiles.buzzsaw.com/warehouse	Tools Edit Refresh	11:25 AM 7/31/01	X

The Autodesk Buzzsaw and Autodesk Streamline applications are monitored from multiple locations throughout the world to identify what users are experiencing. Tracking the response of specific actions shows whether international users are having problems connecting to the server.

Because of the nature of the Internet, not all problems can be corrected immediately; however, users are notified about problems so they can plan accordingly.

Because monitoring alone cannot provide the reliability and availability users depend on, sound operational practices are essential. Autodesk has routines and procedures for

- Incident management: All incidents (alerts) must be responded to and the impact, actions, and recommendations documented. Managers check and approve all incident reports.
- Problem management: Recurring incidents or identified problems are documented and allocated to the appropriate team for corrective action.
- Change management: All changes to systems must go through an approval process.
- Configuration management: Records are kept on all components within our environment.

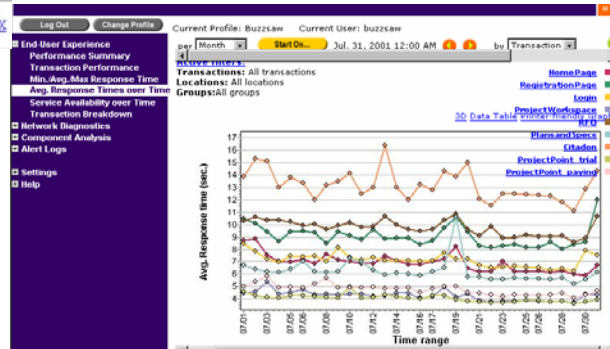
Autodesk processes are based on IT industry best practices as defined in the ITIL Service Support Best Practices, and we are continually improving on them in accordance with industry standards.

Disaster Recovery

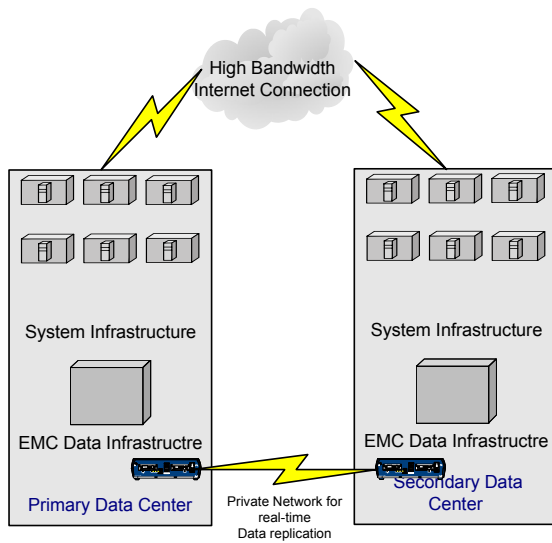
Although Autodesk has implemented redundancy at all levels of the infrastructure, there is always the possibility that the primary data center will suffer a catastrophic event. In extreme cases, it is possible that the data in that data center could be destroyed.

To protect data in the event of a disaster, Autodesk has a business continuance (disaster recovery) data center, in addition to the primary data center. This data center is geographically separated from the primary data center and offers features similar to those of cable and wireless facilities.

In addition to monitoring, we also perform real transactions to ensure that the application is responding to users. The timing and success of these transactions are monitored from one consistent location, and anything outside the acceptable response activates the escalation process for corrective action.



Protecting Your Data: Secure, Stable Project Collaboration from Autodesk



Autodesk has implemented a copy of the primary data center infrastructure, software installation, and all network, server, and data storage equipment so that we can provide service from that location.

To ensure that all user data is available, we replicate all data from the primary data center to the second location in real time. This ensures that all data entered into Autodesk systems before a disaster event will be available after recovery.

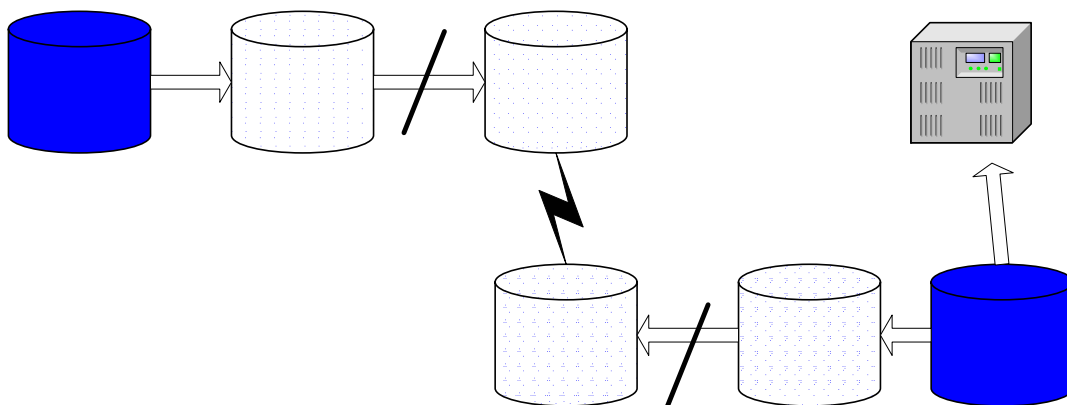
Autodesk uses EMC® data storage technology, recognized as the leader in the field. We use both SAN and NAS technologies to access an EMC Symmetrix frame containing 16 terabytes of storage. The EMC Timefinder and Symmetrix

Replication Data Facility technologies then transfer data to a second 16-terabyte EMC Symmetrix frame.

We replicate more than five terabytes of user data between the two locations. This requires mirroring data within the main frames. In addition, another five terabytes are used to take point-in-time snapshots of all user data, resulting in an instantaneous backup.

This data is then synchronized with the remote data storage and is copied to tape using EMC Data Manager (EDM) and an ATL 3000 tape library.

The tapes are taken offsite daily on a three-month rotation.



Glossary

Cluster: Two or more servers that are connected in a manner that allows the seamless transfer of processing in the event of a fault.

Load Balancing: A network device used to evenly divert system or user requests to multiple servers for processing.

SAN (Storage Area Network): A network that directly attaches large storage systems to database or file servers using a private high-speed network (Autodesk uses a dedicated high-speed fiber-optic network).

NAS (Network Attached Storage): Technology that allows large storage systems to be accessed through common network file-sharing methods (Windows file share). Autodesk uses dedicated data servers to allow connection to high-speed fiber-optic storage networks used by the SAN.

Firewall: A combination of hardware and software, located at the perimeter of a network, that protects resources from users in other networks.

BCV (Business Continuance Volume): Technology used in the EMC storage system to make almost instantaneous copies of large quantities of data without affecting systems or users.

autodesk[®]

Autodesk, Inc.
The Landmark @ One Market
Suite 500
San Francisco, CA 94105
USA

Autodesk, Autodesk Streamline, Buzzsaw, and ProjectPoint are either registered trademarks or trademarks of Autodesk, Inc., in the USA and other countries. All other brand names, product names, or trademarks belong to their respective holders.

© Copyright 2002 Autodesk, Inc. All rights reserved.