HA / DR Jargon Buster

(High Availability / Disaster Recovery)

Term	Definition
Apply Threads	A configuration task that runs within the replication process on the Target system to apply the changes from the Source. Additional apply threads can be configured to run concurrently with other apply threads to manage larger volumes.
Alternate Site	An alternate facility in a location other than where the primary production server is run, that has the equipment and resources to recover the business functions affected by the occurrence of a disaster.
Application Recovery	A key part of disaster recovery is the restoration of business system software and data, after the operating system environment has been restored.
Asynchronous Data Replication	A method (see asynchronous protocol) for copying data between a source and target system while the application continues to process data on the source system. The content of database copies may differ from the original storage site (by fractions of seconds), as determined by the time to transmit the data over a communications network to the alternate site.
Asynchronous Protocol	The asynchronous protocol is the most widely used communications protocol between computer devices and is well suited for geographically dispersed communications. With the asynchronous protocol there is no need to send an acknowledgement of data receipt prior to the changes being saved as there is with the synchronous protocol.
Autonomics	Procedures built into an application that operate organically in response to input from the application to detect, identify and self-heal errors that occur.
Availability	The ability for users to access software applications and data when required. When systems are not available they are experiencing downtime and considered unavailable.
Backup	A copy of the production data and/or system at a point in time. The backup can be a full system, a database, or other portions of data and programs running on a production server environment. The process of creating a copy of data is to ensure against its accidental loss.
Backup System (Target)	A system that is used in place of a primary application system should it be no longer available for use. Replicated changes from a source application system maintains data integrity so it is available for use on the recovery (target) system.
Backup Window	Used to describe the period of time that a system is available to perform a dedicated backup process. During this period (either daily or weekly) processing is stopped so application files are not being updated so as to allow a consistent backup of application data to be taken.
Bandwidth	The data rate (typically expressed in bits per second or bps) that the network can support; also referred to as throughput.
Business Continuity	Business Continuity is focused on allowing a business to continue functioning after and ideally, during a disaster. As opposed to simply being able to recover following a catastrophic event ranging from hardware failures, local power fluctuations and human errors to natural disaster such as hurricanes, floods and pandemics. This is achieved through the deployment of redundant systems and data replication techniques to provide a reliable backup and recovery strategy.

Business Continuity Planning (BCP)	The aim of Business Continuity Planning (BCP) is to make advance preparations to enable business activities to continue after an interruption. The BCP should answer two questions, "What could go wrong?" (risk analysis), and "If something went wrong, how would it affect our business?" (business impact analysis). The BCP plan then answers how the business will continue to function in the event of an outage or system interruption and help determine the recovery strategies for both technology capability and business units.
Business Impact Analysis (BIA)	A management level analysis to identify an organization's exposure to the sudden loss of selected business functions and/or supporting resources (threats), and analysis of the potential disruptive impact of those exposures (risks) on key business functions and critical business operations. The BIA measures the effect of resource loss and escalating losses over time, in order to provide reliable data upon which decisions on risk mitigation and continuity planning can be made.
Cloud HA/DR	Cloud computing is a general term for anything that involves delivering hosted services over the Internet. Cloud (HA/DR) is fully managed service platform that provides data replication infrastructure and software on demand on a subscription payment basis.
Clustering	Two or more computers or nodes networked together which share processing and resources of the connected group. The cluster allows for redundant hardware, software and parallel processing and is often used for high availability.
Colocation Center	An off-site computer processing center where customers locate a server or application. By using this colocation site the individual firms share the benefits of the network, security, availability and experienced personnel for data processing services at a reduced cost compared to providing the same infrastructure individually.
Command Scripting Function	The Maxava HA Command Scripting Function (CSF) provides a framework for customers to enter a series of commands, all associated under a single named description, which will be executed in a similar fashion to a CL program. However the Maxava HA CSF process does not require to be compiled and the commands you enter can be modified directly from the function.
Configuration (CONFIG)	A generic term, used to describe a group of elements of the system and how they are setup or defined to deliver a service component for an application.
Contingency Audit	After the business continuity plan is complete, a necessary check is to perform a contingency audit to confirm dependencies are covered and appropriate procedures are in place. Contingency audits should be conducted regularly to ensure they are up-to-date and applicable.
Continuous Availability	Permanent availability; 100% uptime.
Critical Functions	Critical operational functions and business activities which must be performed in order to satisfy key customers service processes (call center, processing orders etc), and protect the assets or reputation of the company.
DASD	Direct Access Storage Device, i.e. disk.
Data Auditing	Examination and verification of processes and events to ensure data accuracy and integrity for a database that is replicated between a source and target system.
Disaster	A disaster is any sudden, unplanned, severe interruption of normal business activities that causes an inability for a business to provide critical business functions for some extended period of time. It may be caused by a power failure, a computer virus, a system crash or a natural disaster, although human error is a more common cause of a "disaster".

Disaster Recovery (DR)	Recovery of systems and business services after a disaster. Disaster recovery techniques typically involve restoring data to a second (Backup) system, then using the Backup system in place of the destroyed or disabled Primary system.
Disaster Recovery Plan	Thoroughly documented processes, procedures and list of personnel required to recover data processing capabilities for computer operations. The disaster recovery plan outlines the steps to take and documents the systems and application dependencies so that rapid action can be taken to ensure the business systems are up and running as quickly as possible and with little or no data loss.
Downtime	The time that the system and/or applications are unavailable for use.
Fail Over Test	An activity that tests an institution's Business Continuity Plan.
Failover	The capability to switch from a failed Primary system to a standby Backup system without interrupting business operations. Failover can be setup for a component or an entire system. The more important the system/application is to the ongoing business the more important it is to build in failover. See Role Swap.
Fault-Tolerant	The ability of the computer system to degrade gracefully despite the "faults" or failures that might occur with hardware components. Duplicate components are incorporated into the system design which are used if their counterparts fail.
High Availability (HA)	Systems or applications requiring a very high level of reliability and availability. High availability systems typically operate 24x7 and usually require built-in redundancy to minimize the risk of downtime due to hardware and/or telecommunication failures. A system setup that ensures a high degree of operational continuity; generally measured in percentage of uptime in a given year - i.e. four nines (99.99%) annually equals a total down time of just 52.6 minutes a year.
Hot Site	An alternate facility that has the equipment and resources to recover the business functions affected by the occurrence of a disaster.
Journaling	The process of logging changes or updates to a database since the last full backup. Journals can be used to recover previous versions of a file before updates were made, or to facilitate disaster recovery, if performed remotely, by applying changes to the last safe backup.
Latency	The time it takes for a packet of data to travel from one point to another or to return to the sender. For computer networks a low latency is preferable since latency is dependent on the speed of the transmission.
Letter of Engagement (LOE)	A contract that outlines the terms and conditions of services that will be provided, the project scope, responsibilities, deliverables, and deadlines.
Logical Partition (LPAR)	A logical segmentation of a system's resources that allows it to run its own copy of the operating system and associated applications.
Maintenance Window	The time set aside to perform scheduled maintenance for the computer system such as applying software updates. See planned downtime.
Mean Time Between Failures	Mean time between failures (MTBF) is a calculated average between failures of a component or system. The mean time between failures is a way to measure reliability.
Mirroring	Creating an identical, near as possible real-time copy of a component or system on another component or system.

Planned Downtime	The approved scheduled time a system will be unavailable for use. This time is typically used for ongoing maintenance of hardware and software changes and scheduled at regular intervals.
Primary System (Source)	The production or primary server that is used to perform the main application processing functions for a business.
Pseudo Role Swap	Simulating the swap of the primary production environment to the target system to test the data consistency of the target system. A full network swap is not necessarily needed to test the HA/DR software in this instance.
Recovery	The process of rebuilding data after it has been damaged or destroyed. In the case of remote copy, this involves applying data from secondary volume copies.
Recovery Point Objective (RPO)	The point in time to which systems and data must be recovered after an outage. This is the amount of information the business deems acceptable to risk losing or manually recreating.
Recovery Time	The period from the disaster declaration to the recovery of the critical functions.
Recovery Time Objective (RTO)	The amount of time to recover from a system interruption and is measured by the number of hours or days in which a business wants to recover a resource or resume a business activity. The RTO is set based on the risk analysis. The time is based on the full recovery of the system availability to the end users with all functionally restored.
Redundancy	Additional components or systems standing ready to use if the source system or component fails. Built-in redundancy delivers little to no interruption in availability.
Reliability	The ability of the system to perform without interruptions or the probability that the system will perform its intended function(s) over time. This is usually expressed in percentage terms.
Replication	The process of capturing, transmitting and applying all predetermined changes with integrity from a source or primary system to a target or backup system, so that it is kept continually synchronized.
Risk Analysis	The process of identifying and assessing factors that may contribute to the success or failure of a project or goal. The risks involved could have possible threats leading to business vulnerabilities. A risk analysis aims to control the impact of unfortunate events.
Role Swap	The process of automatically moving a primary production server or process from one server or component to a backup/target server or component, in the event that the primary environment is damaged or unavailable.
Role Swap Readiness	This is a state of readiness and comfort level that a role swap can be successfully performed. This is accomplished by regularly testing the role swap process between the Source and Target systems using predetermined procedures.
Service Level Agreement (SLA)	A formal contract or agreement signed between two parties (service provider and the "customer") regarding the level of service provided and how to measure the service level. Penalties are usually invoked if the SLA has been consistently missed over a predetermined length of time.
Single Point of Failure (SPOF)	Any single component in the system that will cause the system to stop functioning if it fails. This usually refers to hardware, but may refer to other critical elements.
Source (Primary)	The production or primary server that is being used actively for business processes and storage of information.

Synchronous Protocol	A operation in which the primary database copy function copies updates to the secondary target database at the same time that the primary volume is updated. The synchronous communications protocol requires that, for each data packet transmitted, the sending program must wait for an acknowledgement of receipt from the receiving program before sending the next message packet. This communications protocol relies on the communications pathway to be efficient and is less effective for larger geographical distances between the sending and receiving programs.
Target (Backup System)	The non-production or backup server which receives the replicated changes from a source server and is kept synchronized with the production system.
Threat	A threat is anything that *could* cause a disaster for a business. Threats can be natural (such as storms), technical (such as computer viruses) or human (such as labor disputes). Creating a business continuity plan will minimize potential losses in the face of a threat.
Unplanned Downtime	Any unscheduled event that leaves the system and/or applications unavailable for use.
Uptime	The time a system is available for use.