Backups – An Overview

V0.3 2021-11-17



Copyright © 2021 Real World Technology Solutions

All rights reserved.

Contents

[1 Backups – An Overview 4](#_Toc88123863)

[1.1 Terminology 4](#_Toc88123864)

[1.2 What is a Backup? 4](#_Toc88123865)

[1.3 Why Take Backups? 4](#_Toc88123866)

[1.4 What to Backup 5](#_Toc88123867)

[1.5 When to Backup 5](#_Toc88123868)

[1.6 Where to Backup 5](#_Toc88123869)

[1.7 Other Considerations 5](#_Toc88123870)

# Backups – An Overview

This document discusses backups and their importance to protecting an organisation’s data and ability to perform its normal operations.

## Terminology

Here are some important definitions.

* Backup (noun) – a copy of something, usually data, kept in a separate location from the original; this could be a separate physical device or a different location on the same device
* Backup (verb) – the process of creating a backup of something (“backed up” after it is done)
* Archive – a backup where the original has been deleted and the backup is now the only copy of the thing backed up
* Shadow or Mirror – a duplicate of data that is updated in real time as the data changes
* Repository – a place where backups and archives are stored, either online or on separate devices physically stored somewhere
* Recovery Point Objective (RPO) – the amount of data that is considered the maximum amount of data loss that is acceptable, normally measured in time; e.g. “no more than one week of data” means an RPO of one week. The RPO defines the maximum time between backups – the actual interval between backups should be shorter than the RPO.
* Recovery Time Objective (RTO) – the maximum amount of time it can take to recover and restore data when required; e.g. “no more than four hours” means an RTO of four hours
* Retention Period – the length of time a backup of data is retained; a retention period of “one year” means backups of data can be discarded after one year from the time of backup.

## What is a Backup?

A backup is a copy of electronic information, made to protect that data against loss or undesirable changes. Typically, organisations have large amounts of data that is essential to their core activities. That data can be lost in a cyber security incident or other disaster, or by accidental changes made by people or bugs in software. If that happens, a backup is likely to be the only reliable way to quickly recover and restore the data affected.

Backups are usually made to disk devices, either within the organisation or somewhere in the “cloud”. Sometimes backups can be made to media like tapes and, very rarely, DVDs.

Importantly, a backup of data must not be available to be used like the original data. A backup is a copy of the original and must remain safe, secure and unused by any normal activities. Although the original may subsequently change, either through deliberate, valid actions, or by undesirable events, the backup is a constant untouched copy that can be used to recover the original data as it was at a specific point in time, if required.

## Why Take Backups?

The simple answer is to protect information and the operations of the organisations that use the data. Cyber security incidents almost always target data. Ransomware is a classic example where data is “hijacked” and made unavailable until demands from the cyber criminals are met, usually in the form of some payment. Backups make such incidents less effective in disrupting business. Lost data means lost business at the very least. It can also result in consequential damage!

## What to Backup

Each organisation should have its own policy on what to backup based on the data it has, and how that data is used. However, there are some basic principles that apply to all organisations:

* Understand what data is stored and used, and how much disk storage space it requires
* Understand how the data is used by the organisation
* Understand the effects and impact if the data is not available when needed
* Know how frequently data changes
* Know how old (i.e. out-of-date) data can be used, if at all, when current data is lost
* Backup critical data and any data where its loss is not acceptable to the organisation

This information forms the basis for decisions on what, when and where to backup data.

## When to Backup

Backups must be taken regularly. That frequency will be different for different data depending on how it is used. This means there will almost certainly be several backups of the same data, taken at different times. This forms an historical record of the data over time. Some general guidelines:

* Take backups automatically, where possible – avoid relying on manual actions
* Schedule backups at an interval that is less than the maximum time period the organisation is willing to let pass where all data in that period is lost – for example, if loss of as much as a month of data can be tolerated, backups might be taken each month; however, if the loss of even a day of data is too much, backups may happen every 12 hours or even more frequently, if warranted
* Where possible, schedule backups at times when the data is unlikely to be in use – this will help to prevent possible data inconsistencies where the data is all valid, but may be only part of the full data update of a particularly complex change in progress; this “quiet period” is often overnight or when users are not logged into systems.

## Where to Backup

Backups can be made to local disk storage, a local tape device, remote storage devices within the organisation, or cloud-based storage from a service provider. Organisations need to have a basic level of skill to ensure backups are taken correctly, verified to have been successful, and can be restored when needed. Some general guidelines:

* Local disk storage is normally convenient and most often used, but there must be sufficient dedicated storage for backups and relevant backup software, and the cost of all that must be understood and accepted
* Local backups need to account for the risks of loss of the original and backups in a disaster
* Remote or cloud-based backups can be used to reduce risks of loss of original and backed up data – they may (or may not) be cost-effective, but they usually offer a higher degree of resilience in a major incident

## Other Considerations

Be sure to understand the purpose of a backup versus an archive of data. Both are legitimate actions to take, but archives are designed to free up the storage space of data that is considered to be archival in nature; i.e. no longer needed for normal operations and therefore not needed to be readily accessible. There is a higher risk of loss of archived data should the archive itself be lost.