Recover a Minecraft server after griefing

Contain the incident before trying to repair it. Restrict access for the accounts involved, preserve evidence and decide whether you need a few builds repaired or an entire server rolled back. Keep a current backup even if it contains damage: it preserves the remaining good work and gives you a way back if recovery goes wrong.

Stop further changes and record the scope

For active destruction, stop the server or temporarily restrict joining through your established access controls. Record approximate times with a time zone, affected worlds and coordinates. Save relevant logs and identify whether the damage came from a player, an exploit, a compromised operator or a plugin.

Review operator and plugin permissions before reopening. If credentials may be compromised, follow the account compromise checklist. Repairing a build while the attacker still has access leaves the original problem unresolved.

Check what recovery evidence exists

CoreProtect can help with actions that it actually recorded and still retains. Installing it after griefing cannot reconstruct earlier events. Logging exclusions, purged history, unsupported actions or unavailable databases can also leave gaps. Check the plugin's status and database before assuming the whole incident is recoverable.

A full backup gives a different recovery point: restoring it also rewinds legitimate changes made after its timestamp. If there is no suitable history or backup, explain the limit to players rather than promising that every item or build can be restored.

Preview a small CoreProtect rollback

1. Verify a current full backup, including the CoreProtect database and other external plugin databases. Test on a separate copy when the incident is extensive.
2. As a trusted operator in game, stand at the affected location in the correct world. Use `/co inspect` to inspect blocks and identify relevant recorded activity; toggle it off afterward.
3. Look up a bounded example, replacing `SuspectName` and the time window with the confirmed incident: `/co lookup u:SuspectName t:1h r:20 a:block`.
4. Preview the same scope: `/co rollback u:SuspectName t:1h r:20 a:block #preview`. Here the radius is centred on your in-game position; do not paste this into the server console expecting the same centre.
5. Read the preview and follow your installed version's confirmation instructions only when its user, time, area and actions match the evidence. Cancel an incorrect preview and narrow the scope.

The block filter does not mean that container contents, inventories or every entity will be restored. Investigate these separately. Avoid global rollbacks and broad time windows that also undo other players' work. CoreProtect's restore operation can reverse recorded rollbacks, but it is not a replacement for a verified recovery backup.

When a backup is the better option

For widespread corruption or changes outside logging coverage, keep the server stopped and compare available backup timestamps with the incident. Agree the lost-progress window with players. Restore a consistent set of worlds and dependent plugin data, then test privately before reopening.

Further reading: CoreProtect commands and preview filters, logging configuration and individual player-data recovery.

Revision #2
Created 2026-11-08 21:28:53 UTC by CloudExa Hosting Admin
Updated 2026-11-08 21:28:53 UTC by CloudExa Hosting Admin