# The Complete Guide to Backup and Recovery for ServiceNow

# Contents

# Why Backup Your ServiceNow Data?

As public sector organizations continue to move processes to the cloud, platforms that serve as the foundation for these initiatives have become increasingly popular—and important—to departments, agencies, and public bodies of all sizes and across all industries.

One example is ServiceNow, which is a cloud-based platform that helps public sector personnel quickly and efficiently digitize workflows and run them at scale. Focusing on digitizing processes, ServiceNow creates efficiencies across operations  to deliver better citizen outcomes.

While companies like ServiceNow provide cloud platforms with proven infrastructure far beyond what most enterprises can achieve with on-prem solutions, data resiliency and security need to remain in clear focus for all public sector organizations using cloud services, especially as a growing number of business processes and workflows transition to these platforms.

# A Shared Responsibility for Keeping Data Safe

As with most other SaaS providers, ServiceNow customers bear ultimate responsibility for protecting all the data they have stored on the platform.

The shared responsibility model states that Cloud Service Providers (CSPs) are responsible for security of the cloud, and customers are responsible for security in the cloud:

- **CSPs**

  Responsible for configuring, managing and securing applications, network controls and the host infrastructure.

- **Customers**

  Responsible for all data stored in the cloud, endpoints (devices), and account and access management.

# How Does Data Loss and Corruption Happen in ServiceNow?

Within any cloud environment, there are disruptive events that can impact data availability and security in the cloud:

- Data corruption or deletion caused by a bug or human error
- Upgrade or maintenance errors that occur during planned maintenance
- Malicious attacks that successfully delete data or databases

It's also important to remember the vast majority of data loss and corruption issues aren't tied to major events. Simple mistakes happen every day, like:

- Migration errors when moving large volumes of data, consolidating data, or importing data
- Developers or admins releasing applications, workflows or system updates into production without proper testing
- Errors in integrations that inadvertently corrupt data

Significantly, 78% of ServiceNow users experiencing data loss or corruption are unable to recover all their data.

SAAS DATA PROTECTION: A WORK IN PROGRESS, ENTERPRISE STRATEGY GROUP, 2022

# ServiceNow Backup Options

## Periodic Full Backups

As part of ServiceNow's Advanced High Availability Architecture, ServiceNow creates regular full backups of the platform. Here are important aspects of full backups that have an impact on their utility for restores:

- Full backups are performed every **seven days** (weekly) and differential backups are taken every 24 hours (daily).
- ServiceNow keeps **two weekly** backups and **six daily** backups.
- Weekly backups are retained for **a maximum of 14 days** and daily backups are retained for **a maximum of 7 days**.
- Customers do not have control over the exact timing of backups. The system finds the best time for backups.

## Record Auditing

ServiceNow also offers the ability to enable auditing on tables. When auditing is enabled a log of record creation, updates and deletion is maintained in an Audit table and History set table. The information in these audit tables is used as the basis for the Deleted Records and Delete Recovery Modules that enable rollback of deletions.

Source:

https://www.servicenow.com/content/dam/servicenow-assets/public/en-us/doc-type/resource-center/white-paper/wp-sn-advanced-high-availability-architecture.pdf

https://support.servicenow.com/kb?id=kb_article_view&sysparm_article=KB0678054#q8

https://support.servicenow.com/kb?id=kb_article_view&sysparm_article=KB0724183

https://docs.servicenow.com/bundle/rome-platform-security/page/administer/time/concept/c_AuditedTables.html

# ServiceNow Recovery Services

## Restore Entire Instance From the Full Backup

A full instance restore can be completed by requesting it from ServiceNow support. There are limitations in how far back the restore can be conducted, the granularity of the restore, and the amount of time it will take to complete the full instance restore. These limitations are further detailed below.

## Deleted Records Module

This module works on records in audited tables and is only suitable for data loss, not data corruption. In addition, recovery of cascaded deleted records must be done within seven days of the record deletion.

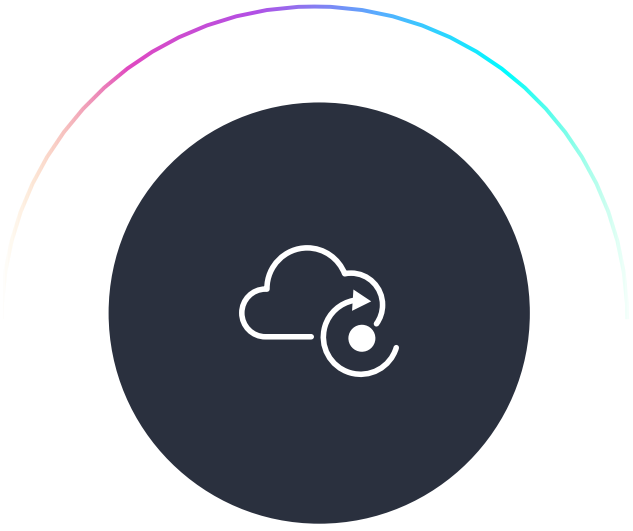
To find this module, navigate to **System Definition > Deleted Records**.

## Delete Recovery Module

This module works for any deleted record, and is also not suitable for data corruption. It is also not available for every underlying type of database. This recovery must be done within seven days of the record deletion. To find this module, navigate to **Rollback & Recovery > Delete Recovery**.

## Script Execution History Module

This module works on scripts executed using the Scripts - Background module. This history only includes seven days of script executions. To find this module, navigate to **Rollback & Recovery > Script Execution History**.



Source:

https://docs.servicenow.com/en-US/bundle/sandiego-platform-administration/page/administer/table-administration/concept/rollback-delete-recovery.html

# Limitations of ServiceNow Backup and Recovery

## Data Backup and Recovery Limitations

Despite ServiceNow's Advanced High Availability (AHA) architecture, they do acknowledge that, in certain scenarios, it may be desirable to use more traditional data backup and recovery mechanisms:

> ServiceNow's Advanced High Availability (AHA) architecture is the primary means to restore service in the case of a disruption that could impact availability. However, in certain scenarios, it may be desirable to use more traditional data backup and recovery mechanisms. Such circumstances could be, for example, where a customer deletes some data inadvertently, or where a customer's data integration or automation is misconfigured or malfunctions, resulting in data being rendered unusable or inaccessible. In these scenarios, the high availability capability would not assist and restoring frombackup is the only option for recovery.
>
> ADVANCED HIGH AVAILABILITY ARCHITECTURE, SERVICENOW

Despite ServiceNow's Advanced High Availability (AHA) architecture, they do acknowledge that, in certain scenarios, it may be desirable to use more traditional data backup and recovery mechanisms:

- **Retention Periods**

  Within ServiceNow, you can retain weekly backups of your production instance for up to 14 days, and daily backups for 7 days, periods which you cannot extend.

- **Speed of Restore**

  To recover your data, you need to work with ServiceNow support, which could take up to several days, depending on the size of your environment and whether you need to restore data in a granular fashion.

- **Granularity**

  Restore processes are designed to replace an entire database. Recovering specific data only requires additional steps that will further delay the entire restore process.

  For these reasons, ServiceNow recommends avoiding restoring a production instance from backup and only doing it as a last resort.

Source:

https://www.servicenow.com/content/dam/servicenow-assets/public/en-us/doc-type/resource-center/white-paper/wp-sn-advanced-high-availability-architecture.pdf

## Module Limitations

The other options to restore data are to use the Deleted Records, Delete Recovery modules or - when the unwanted changes are based on script execution - to use the Script Execution History module.

As noted above, both the Delete Record module and Delete Recovery module are limited only for addressing data loss, not data corruption. While the Delete Recovery module enables recovery of records with relationships, that's only possible for 7 days. The Deleted Records module does not have the 7 day limit. Instead the limit for how far data can be rolled back depends on whether the needed information is still in the audit records. The Delete Records module is also limited in that it won't restore record relationships.

For restoring data corruption, directly querying the audit tables and building custom scripts is possible, assuming the corruption is not from an import set or upgrade. Using scripts can be impractical, however, because creating them can take time away from other development efforts and their execution can be slow due to long running queries and errors in scripting could leave some data unrestored.

"ServiceNow customers, like all SaaS users, must take ultimate ownership for the availability and accuracy of the data that drives their businesses. This means being proactive and having automated backups and granular recovery tools that can meet the business requirements for continuity. When the capabilities offered by SaaS providers cannot meet these requirements, solutions like Own can help customers ensure theirdata is resilient."

**PHIL GOODWIN**
**RESEARCH VICE PRESIDENT, IDC**

# Own Recover for ServiceNow

While ServiceNow does offer some native backup and recovery capabilities, Own Recover for ServiceNow, powered by AWS, equips public sector organizations to better address data resiliency and compliance concerns with capabilities such as the retention of daily backups for up to 10 years, proactive notification of unusual data loss or corruption, and the ability to restore data - from the entire instance down to individual records - in self-service. Plus, 100% of data is stored in AWS, which is architected to be the most flexible and secure cloud computing environment available today.

## Module Limitations

### Gain peace of mind during changes to your instances

Run on-demand backups before and after significant changes to your instances such as upgrades, migrations, new customizations, and integrations. Compare pre- and post-change backups to verify there's no unexpected data loss or corruption.

### Protect your growing SaaS footprint with a single solution

Manage backups from additional applications like Salesforce and Microsoft Dynamics 365 through the same pane of glass. Tap into a comprehensive platform of Own data protection solutions that span data security, archiving, and seeding.

### Stay audit-ready with searchable archives of historical data

Protect yourself against the risk of unwanted deletion or corruption of vital information. Answer questions about past history using keyword searches across backups, files, and attachments.

### Ensure regulatory compliance

Tailor retention policies for every instance to keep immutable copies for exactly the right time period. Retain daily backups for up to 10 years and monthly backups for up to 99 years.

### Restore only what's needed, quickly

Quickly zero in on changed tables, items, and fields using visual tools. Easily identify which changes are unwanted. Accelerate data recovery by choosing specific records and specific fields and initiating restore with the click of a button.

### Use backup data to feed analytics

Export historical backup data to feed analytic data stores. Schedule daily exports to automatically keep data up to date.

### Ensure the accuracy of platform data

Analyze historical patterns of changes to items and pinpoint when unwanted loss or corruption may have occurred. Get notified about unusual levels of data changes and deletions.


OWN YOUR OWN DATA

## About Own

Own is the leading data platform trusted by thousands of organizations to protect and activate SaaS data to transform their businesses. Own empowers customers to ensure the availability, security and compliance of mission-critical data, while unlocking new ways to gain deeper insights faster. By partnering with some of the world's largest SaaS ecosystems such as Salesforce, ServiceNow and Microsoft Dynamics 365, Own enables customers around the world to truly own the data that powers their business.

It's their platform. It's your data. Own it.

Learn more at owndata.com.