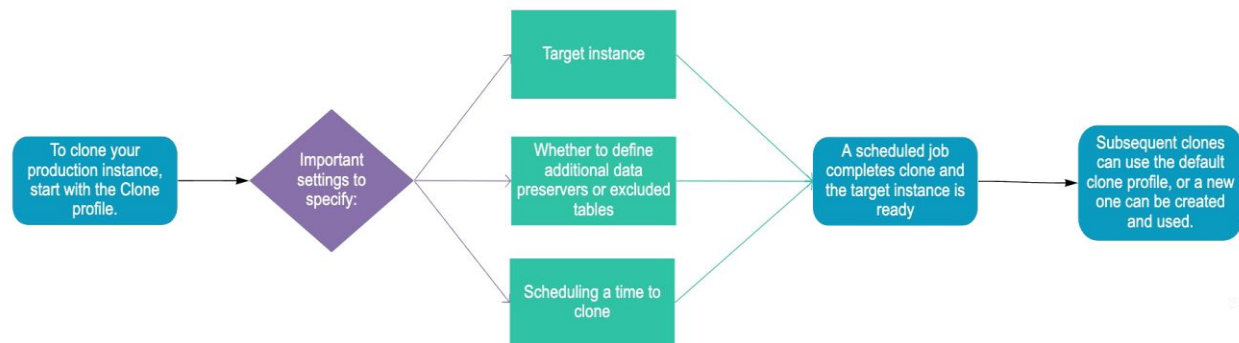# System clone in ServiceNow

- This application is used to copy everything in a database from one instance to another.
- Cloning is typically used to copy a production instance to a pre-production instance to test changes.
- Cloning data comes from the most recent, nightly backup.

Clone Process

In response to a clone request, the ServiceNow platform performs the following tasks:

1. Generates a file to preserve operational data on the target server.

Note: This file contains the data preserved by data preservers.

Sometimes, it is necessary to preserve some data on an instance targeted for cloning. For example, if the target is a MID Server, you must not overwrite the MID Server [ecc_agent] table. Preserved data is stored on the target instance before cloning begins and is restored on the target instance after cloning.

2. Copies the database schema from the source instance to the target instance.

(create a record of Request clone by selecting the clone profile, target instance and clone scheduled start).

3. Creates tables in the target instance database using the source instance table definitions.
4. Copies data from the most recent nightly backup of the source instance to the target instance database.

Note: Certain exclusions are automatic, large tables are normally excluded. These include audit, log, and email tables. MetricBase tables are not excluded by default.

5. Briefly disables UI traffic and requests to the target instance server.
6. Displays the message **Clone in progress...** to any user accessing the target instance.

7. Restores operational data preserved from the target instance.
8. Runs any post-clone cleanup scripts on the target instance.
9. Briefly suspends all email functions on the target instance.
10. Queues an event to regenerate text indexes.
11. Enables UI traffic and requests to the target instance server.

During a clone, the target instance may be intermittently unavailable. After clone completion, you have up to 24 hours to contact Customer Service and Support and request a rollback of the target instance to its pre-clone state. You are notified when the rollback is complete.

Note: If the source instance has a clone depth level of >=5 then the clone is not allowed.

If the source instance purpose is DART (Data Access for Responsible Training) then the clone is not allowed, and an error message will be displayed.

Note:

Preserve means: keep what data is already there on the target instance but add to it.

Exclude means: If no preserve, don't even bring data to the target instance, but instead make it empty. Otherwise, if preserved, but excluded, then keep what is there, but don't touch it.

Clone to an instance on a different version

The System Clone application can target an instance running a different instance version from the source.

A central web service controls clone processing and automatically modifies the target instance version to match the source instance version. This matching process starts up to 8 hours before the time specified in the **Date and time** field on the System Clone form. This web service also ensures that there is enough disk space on the target instance for the clone to proceed.

When cloning from a backup, the target instance does not need additional time to upgrade or downgrade. The ServiceNow platform performs any version changes during a brief window where the target instance is unavailable, after it copies data from the source instance backup.
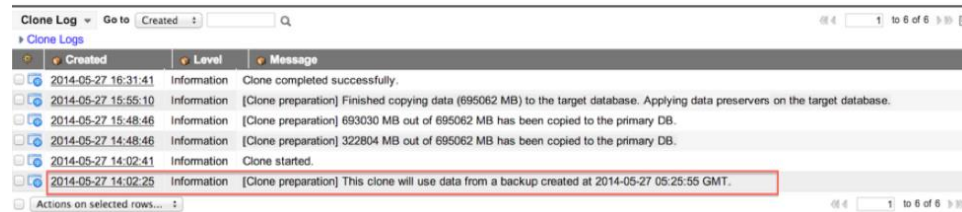
Clone from a backup

The Now Platform uses data from the most recent, nightly backup of the source instance when cloning. Backups that are used for cloning are a maximum of 36 hours old. System Clone begins the initial preparation, including selecting the latest backup to use, only at the date and time processing is scheduled to start.

If cloning from a source backup fails, the system uses the legacy clone engine instead. The legacy clone engine cannot preserve data from extended tables, relationships, hierarchies between tables, and dot-walked queries. You may want to restore the target instance from a backup and then reschedule the clone in such cases.

After cloning from a backup, the target instance is unavailable for several minutes before the clone is marked as complete in the source instance. If the source and target instances are on different versions of the Now Platform, the target instance is modified to match the source instance version during this time.

When starting a clone from a backup, the date and time the backup was taken, as well as periodic progress messages, appear in the **Clone Log** related list.

System clone backup log

Clone over production instances

As long as the system property, glide.db.clone.allow_clone_target is TRUE, an instance can serve as a clone. Modifying data on the source instance during a clone can cause a data mismatch between records or duplicate record entries.

Clone Admin Console

The Clone admin console provides admins with an overview of their active clones and clone statuses. A new and improved UI for system clone is introduced in the Vancouver release. For more information, see Clone Admin Console. The benefits of the new Clone Admin Console are as follows:

- A simplified clone request experience.
- A new scheduling tool to prevent timing conflicts.
- An on-demand backup option.
- The ability to see all clone-related settings in one place.
- Enhanced visibility via a dashboard to easily view current clone activity.

Request a clone
Request a clone to copy data from a production instance to a non-production instance or to copy data between non-production instances.

Cancel a clone
You can cancel requested, scheduled, and active clones without negatively impacting system stability or usability. Canceling a clone restores the target instance to the pre-clone state, retaining all original data.

Schedule cloning
You can use System Clone to schedule automatic cloning, which is the easiest way to keep your cloned instances up to date.

Modify cloning schedules

You can cancel scheduled cloning but not modify them.

View clone status

You can view the status of a clone to make sure the cloning process isn't stuck.

View clone history

You can view the status and history of any system clone request.

Roll back a clone

Return a clone target to its state before the latest cloning. Roll back cloning if something went wrong in the cloning process.

Post-clone cleanup scripts

Cleanup scripts automatically run on the target instance after the cloning process finishes.

Clone Admin Console

The Clone admin console provides admins with an overview of their active clones and clone statuses. A new and improved UI for system clone is introduced in the Vancouver release.

Request Clone:

Create a clone target

A clone target record specifies the instance URL and credentials used for cloning.

- provide credentials for a user with the admin role. Use a local user account, not an LDAP or SSO user account. The target instance credentials must exist in the User [sys_user] table as a user record or as part of an LDAP integration. Clone requests cannot redirect authentication requests to a single sign-on identity provider.
- System property on target instance: verify the system property glide.db.clone.allow_clone_target is set to **True**. By default, this property is enabled on instances whose name ends in Dev, Test, Stage, UAT, or QA.
- IP Access controls on target instance: if the target instance uses IP range based authentication, it must allow the IP range 10.0.0.0/10.255.255.255 to communicate on a local network.
- Role required: clone_admin or admin.
- Navigate to All -> System clone -> Clone Target.

Exclude a table from cloning

Exclude a table to create an empty but usable table on the target instance.

Role required: clone_admin or admin

The **System Clone** > **Exclude Tables** module lists the tables that are not copied during a system clone. By default, the system excludes tables for logging, auditing, notifications, workflow contexts, and license usage.

Navigate to **System Clone** > **Exclude Tables**.

You can use data preservers to protect data on the target instance from being overwritten. If you have custom applications, you must also manually preserve unpublished application content.

Warning: You must define data preservers on the source instance. Defining them on the target instance does not preserve the data.

Data preservers typically preserve system settings and themes, such as:

- Instance-specific authentication settings
- Bookmark [sys_ui_bookmark]
- Recent Selection [sys_ui_recent_selection]
- User Preference [sys_user_preference]

Note: A clone does not support preserving data from a database view.

Do not use data preservers to transfer large sets of data, such as user groups. If you must preserve table data, such as users, groups, and roles, consider exporting the records to a file and importing them after cloning.

Navigate to **System Clone** > **Preserve Data**.

Warning: If the clone from backup fails for some reason, the clone process fails over to the legacy clone engine. The legacy clone engine cannot preserve data from extended tables, relationships, hierarchies between tables, and dot-walked queries. You may want to reschedule a system clone or manually transfer data in such cases.

Clone profiles for clone requests in Core UI

A clone profile enables you to store predefined target and clone options. The clone profile automatically populates your clone request with your selected profile settings.

Navigate to **System Clone** > **Clone Profiles** to view your clone profiles.

Cancel a clone

You can cancel requested, scheduled, and active clones without negatively impacting system stability or usability. Canceling a clone restores the target instance to the pre-clone state, retaining all original data.

Role required: admin

Procedure

- Navigate to **All** > **System Clone** > **Live Clones** > **Active Clones**.

The system displays the list of currently active clones.

- Select the clone you want to cancel.

The system displays the System Clone record.

- From **Related Links**, click **Cancel Clone**.

The **Cancel Clone** modal displays.

- In **Specify Reason**, select a reason for the cancellation and click **OK**, or select **Others**, enter a reason in the text box and click **OK**.

The system stops any current clone activities and sets the **State** to **Canceled**.

Schedule cloning

You can use System Clone to schedule automatic cloning, which is the easiest way to keep your cloned instances up to date.

Role required: admin

Procedure

- Click **System Clone** > **Active Clones** > **<one-of-your-clones>**.

Note: (Optional) if the **Options** panel is not already displayed.

Click the **Options** arrowhead so it turns downward.
The **Options** panel appears.

- **Note:** A target instance must be selected, or an error message appears.

Select the **Conflict calendar** to view a calendar with their current clone time and potential conflicts if you want to schedule for a different time.

The conflict calendar appears in a new tab.

- Enter values in the following fields to schedule automatic cloning.

Field	Description

Clone frequency	Defines how often this target automatically receives clone data and the maximum number of occurrences.
	    ○ Weekly – The maximum number of occurrences is 5.
	    ○ Bi-Weekly – The maximum number of occurrences is 3.
	    ○ Monthly – The maximum number of occurrences is 2.

No. of occurrences	Specify the number of automatic cloning. The maximum value you can enter depends on the value selected for the clone request in the **Clone Frequency** field.

- Click **Submit**.

The system displays the **Authenticate Target** modal.

- Enter the **Username** and **Password** for an administrator account on the target instance and click **Authenticate**.

The System Clone form displays the target clone.

- To see the cloning schedule for this target, click the **Recurring Clones** tab.

Each line in the list shows a separate, scheduled cloning session.

- To see log messages for past cloning on this target, click the **Clone Log** tab.
- To see cloning schedules for all the clones in the system, click **System Clone** > **Live Clones** > **Clone History**.

The **System Clones** page lists all the cloning instances in the system along with their scheduled cloning.

Roll back a clone:

Return a clone target to its state before the latest cloning. Roll back cloning if something went wrong in the cloning process.

Role required: admin

Rollbacks remove the latest cloning updates on a cloning target. You can only roll back the latest cloning updates. Rollbacks must occur no more than seven days after the cloning.

Note: Rollbacks must occur no more than two days after the cloning for users with sharded instances.

Procedure

- Navigate to **All** > **System Clone** > **Live Clones** > **Clone History**.
- Select the clone to roll back.
- Under **Related Links**, click **Rollback**.
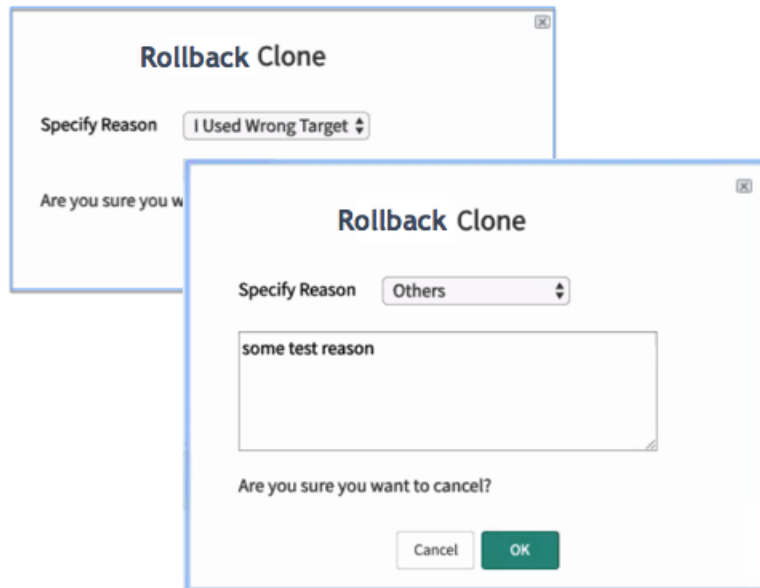
The **Rollback Clone** modal displays
- In **Specify Reason**, select a reason for the rollback and click **OK**, or select **Others**, enter a reason in the text box and click **OK**.

The system rolls back the clone and sets the **State** to **Rollback Requested**, and, if successful, to **Rolled Back**, or, if unsuccessful, to **Rollback Failure**.

You can retry a rollback but if you get repeated failures, contact ServiceNow Customer Support.

Result

The instance contains the same data it had before the clone was applied.

Post-clone cleanup scripts:

Cleanup scripts automatically run on the target instance after the cloning process finishes.

Use cleanup scripts to modify or remove bad data. Cleanup scripts run after data preservers and the clone is complete.

You can add new post-cloning scripts on the source instance to perform any action that can normally be accomplished through script includes or business rules. To add a script, navigate to **System Clone** > **Clone Definition** > **Cleanup Scripts** and click **New**.

Note: Cleanup scripts will always run on clones created using a Clone profile, this is necessary as they're available OOB and ensure a healthy state post clone.

You can make post-clone scripts active or inactive to control whether these scripts run or do not run. You can also set an order number on each script, which enables you to set the order that the active scripts run, with lower numbers having a higher priority.

		Name	Active ▼	Script	Order
☐	ⓘ	Regenerate all text indexes	true	new GlideTextIndexEvent().indexAllNoPurg...	100
☐	ⓘ	Disable emails	true	gs.setProperty("glide.email.read.active"...	300
☐	ⓘ	Install deactivated plugin	true	var separationExceptionFieldProperty = g...	200
☐	ⓘ	Bad MID Server credentials after clone	false	new BadMIDCredentialAfterClone().schedul...	800
☐	ⓘ	Clean Non-Existent MIDs From Application	false	var doesMidExist = function(midSysIdToCh...	700
☐	ⓘ	Schedule drop backup tables	false	if ('true' == gs.getProperty("glide.db.c...	600
☐	ⓘ	Clear scheduled job node association	false	var names = []; names.push('Clean logs'...	250
☐	ⓘ	Configure Email Accounts	false	if (GlidePluginManager.isRegistered('com...	900

The following post-clone cleanup scripts perform various actions on the target instance.

Post-clone cleanup scripts

Script	Description
Bad MID Server credentials after clone	Runs a script include called BadMIDCredentialAfterClone on a cloned instance to detect bad MID Server user credentials. This script include creates scheduled jobs that log MID Servers in the **Down** state to the MID Server Issue [ecc_agent_issue] table after an instance clone.
Clear scheduled job node association	Resets any scheduled jobs that were active on the source instance to the **Ready** state. This script also clears the value of the **System ID** and **Claimed by** fields on all scheduled jobs.
Configure Email Accounts	Migrates email accounts that existed on the source instance to the target instance if they are not enabled there. This script also

	migrates the email properties to the target instance.
Disable emails	Disables email on the target instance. A default data preserver maintains other email settings from the target instance.
Install deactivated plugin	Enables the Domain Separation plugin for instances that use this feature.
Regenerate all text indexes	Rebuilds text indexes on the target instance after a clone. Text indexes are not cloned from the source to the target instance.
Schedule drop backup tables	Schedules the deletion of the data that is contained in the target instance database prior to the clone. This original data is preserved for 24 hours following a clone to enable you to roll back an instance to the pre-clone state. If the target instance is downgraded as part of the clone, backup data is not available.