# Linux Servers Patching – Overview

Monthly patching and regular maintenance of Linux servers using Azure Automation Update management is essential in keeping the Linux server infrastructure healthy in the Oracle Cloud Infrastructure (OCI), up to date and optimized.

The following is a step-by-step guide which is used by the Celero Infrastructure Server Team during Linux patching:

**Simplified Patch Management:** Azure Automation Update Management provides a centralized platform to manage and schedule Linux server patches. Simplifies the complex process of identifying, downloading, and applying updates.

**Enhanced Security:** Monthly patching ensures that your Linux servers are up to date with the latest security fixes. Reduces the risk of vulnerabilities and potential security breaches.

**Compliance and Reporting:** Azure Automation Update Management provides detailed compliance reporting. Helps demonstrate compliance with industry regulations and internal policies.

**Create a patching and maintenance schedule:** Establish a specific date and time each month for performing patching and maintenance activities. Choose a time when server usage is low to minimize user disruption and application downtime. Communicate the schedule to relevant stakeholders, ensuring everyone is prepared for the planned maintenance window.

**Plan for testing and staging:** Before applying patches to production servers, deploy the patches in the (QA/NPD/Sandbox) environments. This environment should closely resemble the production environment, thus allowing you to validate the patches' compatibility and ensure the stability of applications and services post-patching. Test all patches on a subset of non-production servers to identify any issues or conflicts before deploying them to production.

**Reduced Downtime and Disruption:** To apply patches to the QA/NPD/Sandbox environments in OCI (Oracle Cloud Infrastructure). we adhere to the following schedule:

Linux server patching takes place on the 2nd Saturday following the 2nd Tuesday.

For Production servers, we follow a slightly different schedule:

Production server patching is scheduled for the 3rd and 4th Saturday following the 2nd Tuesday."

We follow the above Patching maintenance windows to minimize user disruption. Automated processes reduce manual errors and the risk of service interruptions and Communicate the schedule to relevant stakeholders, ensuring everyone is prepared for the planned maintenance window.

**Review patch releases:** Stay informed about the latest patches and updates released by Red Hat or Oracle Linux, regularly review the Red Hat Customer Portal, errata advisories, and security bulletins to understand the significance of patches and their potential impact on OCI Linux server environment. Consider factors such as security vulnerabilities, bug fixes, and performance improvements when evaluating the need for patching.

**Monitor patching progress:** Monitor the patch deployment progress using the reporting and monitoring capabilities of Azure Automation Update management. Track the status of patch installations, verify successful deployments, and identify any failed or pending updates. Regularly review compliance reports to ensure all targeted servers are up to date and compliant with the desired patch levels.

**Perform post-patching validation:** After patch deployments, perform post-patching validation to ensure that Linux servers are functioning correctly. Test critical Business applications and services to verify their functionality and validate that the server configurations have not been adversely affected. If any issues are identified, troubleshoot and correct them promptly.

**Document patching activities:** Maintain detailed documentation of the patching activities performed on each Linux server. Record the patches installed, dates of installation, any issues encountered, and their resolutions. This documentation serves as a reference for audits, troubleshooting, and tracking the overall patch management process.