SOMR HPC Change Management Guide

Rebecca Tucker - 2024-12-05 - Research Systems

SOMR HPC Change Management Guide

Guiding Definitions: IT Analyst ITSM Client Reference Guide

In Scope

- System-level operating system upgrades
- Storage system configuration changes (hardware, firmware, etc.)
- Changes to firewalls/communications
- Changes to configuration of user-facing nodes
- Compiling of system software affected by the updated kernel

Out of Scope

- Software installation in user home directories
- Creation of new user accounts
- Creation of new directories
- Compute node additions/removal

System of Record: RamsCentral - VCU IT Service Desk Analyst role

Types of changes expected

- Preapproved Changes (using a pre-approved template)
- Planned Changes (changes outside the maintenance window, but non-emergency)
    - Typically Risk Level 2
    - Requires manager approval
- Emergency Changes (atypical)
    - Entered after the change has occurred

    - DOES NOT require manager approval prior to submitting
    - DOES require manager review, once executed in RamsCentral

Maintenance Window

- 1st Friday of the month from 1:00AM - 12:00PM
- Bi-annual maintenance windows for general maintenance & cleanup
- Emergency changes handled on a case-by-case basis

Communication plan

- Using an auto-generated listserv from permission group, an email notification will be sent to inform users of planned maintenance or any emergency changes.
- Patches will be applied based on the identified schedule and/or maintenance window; at that time, technicians will make a determination regarding patches affecting the kernels.
    - If a kernel requires patching for security reasons, that will be handled on an individual basis.
    - By default, we're excluding patches that contain certain file names:
        - CentOS: (exclude=kernel* ibutils-libs* lustre* kmod*)
        - Rocky Linux: (exclude=kernel*,mlnx*,kmod*,lustre*)

Standard entries for RamsCentral fields

Details tab

Summary: Monthly HPC standard patching

Owner:

Team: SOMTech Research Systems

Type:

Emergency: failed hardware on user-facing nodes, etc. (atypical)

Planned: a foreseen change scheduled in advance, but does not fall under the preapproved change template

Preapproved: monthly security patches, as approved via a single planned change (approval of template)

*select template from drop-down

Change Approver: Brian Bush

Category: Operating System

Start Date:

End Date:

Outage Possible:

No - routine OS patches

Yes - High risk changes

Checkboxes: Visible In Portal/Calendar

Public Description:

Preapproved: Apply monthly patches to operating systems and installed applications

Emergency: dependent on purpose of ticket

Planned: dependent on purpose of ticket

Implementation Plan:

Automation software sends available packages for install; technician identifies and verifies necessary patches for upgrade; technician reviews available (but not required) patches and upgrades as appropriate.

Testing Plan:

Necessary patches implemented on node first, then propagated to entire system.

Closure Notes: to be entered once the change has been completed

Technical Description:

Apply monthly patches to operating systems and installed applications; routine maintenance.

Communication Plan:

Preapproved & Planned: No communication is sent for routine maintenance; in a system-down (emergency) situation, an email is distributed to all users.

Recovery Plan:

Uninstall the patches to revert to the prior state.

Risk Details tab

**Note: Specific to Preapproved change; Planned and Emergency may differ.*

How many steps will the change require?

< 5 steps

How many times has the implementation team performed changes similar to this?

> 10

Are any other units involved in making this change or are there any related changes involving different activities?

No

What is the profile of the system undergoing this change or maintenance?

Enterprise / University-wide

When will this change occur? (*Peak dates include registration periods, start and end of the semester, parking permit sales, grant submission and deadlines, etc.)

Business hours on non-peak dates

Was this change tested on a test system?

No

How long will there be a service disruption?

< 5 minutes

Can this change potentially affect the availability, integrity and security of other IT systems?

No

Does this change reduce the security posture of the system, keeping in mind transmission, storage and access to category 1 or 2 data?

No

Is this change occurring during a scheduled maintenance window?

Yes

In the worst case scenario, how long would it take to back out of the change and restore the affected systems to previous settings if the change is not successful?

< 1 hour

When all fields have been satisfied, click the link to send the ticket for approval.

*__Notes:__

1. The Risk Level is determined by the system based on the information supplied
2. If changes/updates are required after the ticket has been submitted for approval, the Change Approver must “Deny” the ticket, returning it to the creator. Updates should be made and then saved. After saving, the ticket may be resubmitted for approval.