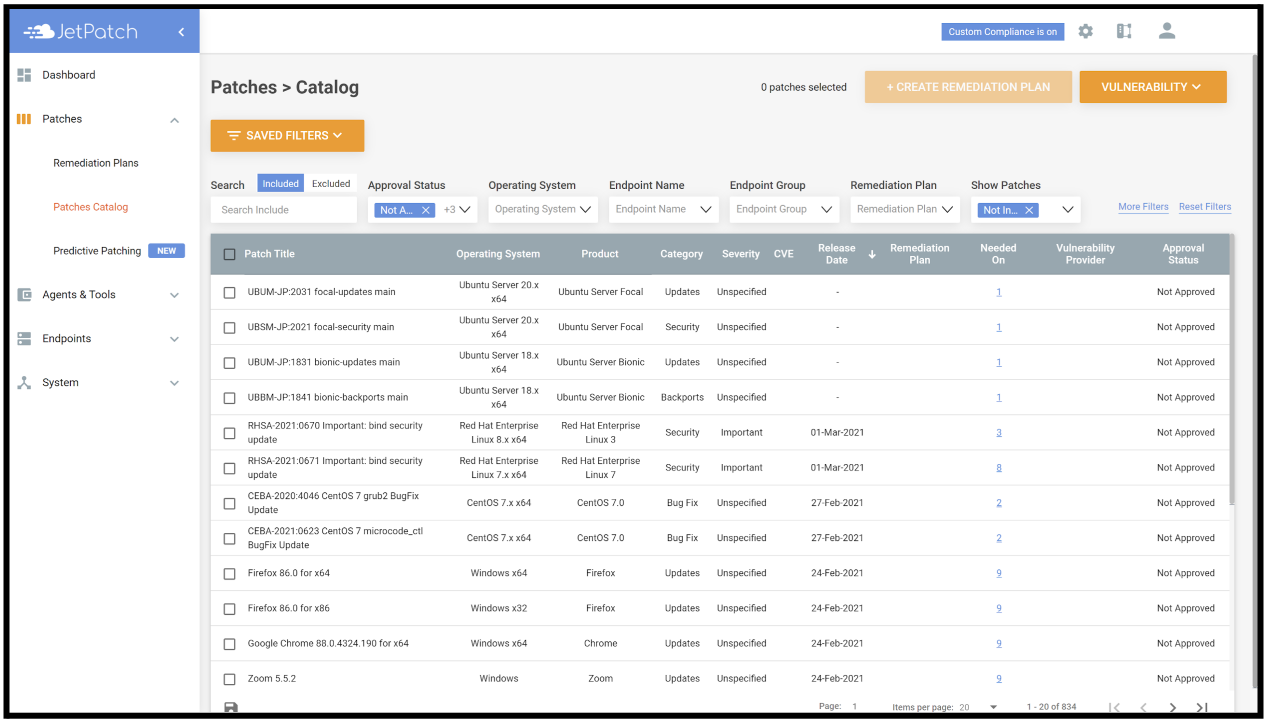
Jetpatch FAQ Guide

Table of Contents

How do I set a Baseline for my Endpoints Compliance?



Patches > Catalog

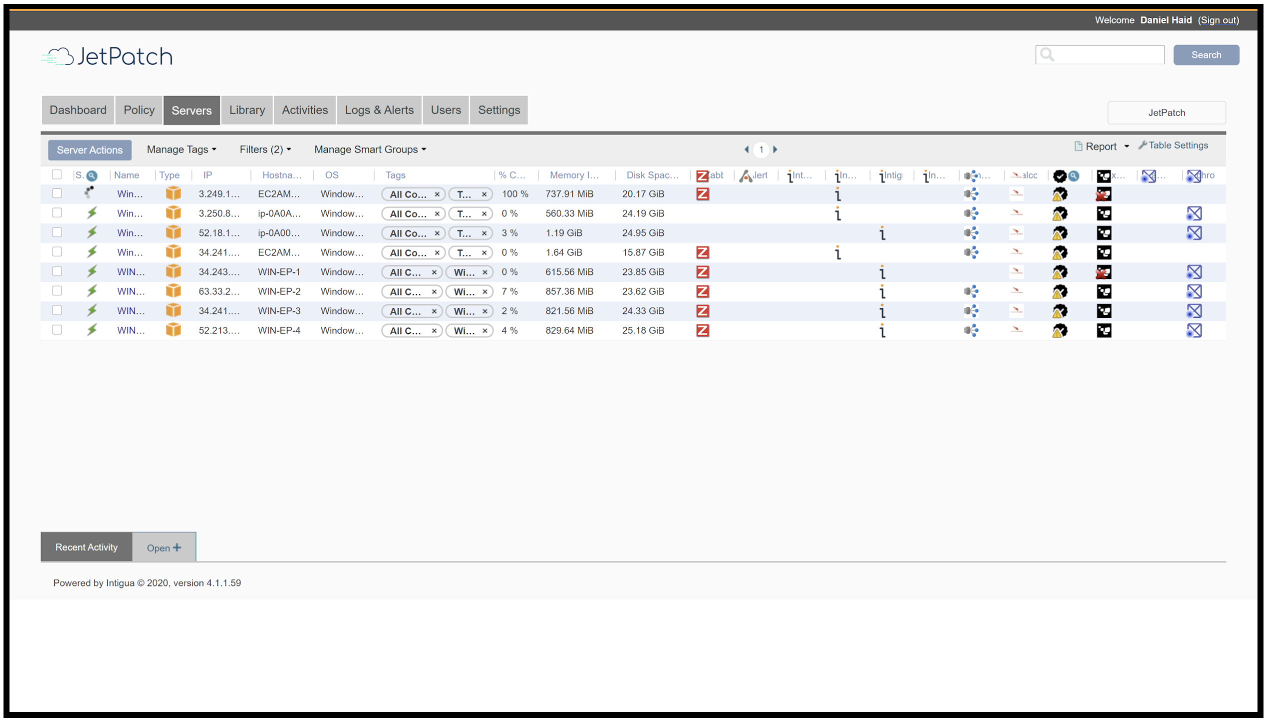
0 patches selected

Search: Included / Excluded — Search Include
Approval Status: Not A... +3
Operating System: Operating System
Endpoint Name: Endpoint Name
Endpoint Group: Endpoint Group
Remediation Plan: Remediation Plan
Show Patches: Not In...

Patch Title	Operating System	Product	Category	Severity	CVE	Release Date	Remediation Plan	Needed On	Vulnerability Provider	Approval Status
UBUM-JP:2031 focal-updates main	Ubuntu Server 20.x x64	Ubuntu Server Focal	Updates	Unspecified		-		1		Not Approved
UBSM-JP:2021 focal-security main	Ubuntu Server 20.x x64	Ubuntu Server Focal	Security	Unspecified		-		1		Not Approved
UBUM-JP:1831 bionic-updates main	Ubuntu Server 18.x x64	Ubuntu Server Bionic	Updates	Unspecified		-		1		Not Approved
UBBM-JP:1841 bionic-backports main	Ubuntu Server 18.x x64	Ubuntu Server Bionic	Backports	Unspecified		-		1		Not Approved
RHSA-2021:0670 Important: bind security update	Red Hat Enterprise Linux 8.x x64	Red Hat Enterprise Linux 3	Security	Important		01-Mar-2021		3		Not Approved
RHSA-2021:0671 Important: bind security update	Red Hat Enterprise Linux 7.x x64	Red Hat Enterprise Linux 7	Security	Important		01-Mar-2021		8		Not Approved
CEBA-2020:4046 CentOS 7 grub2 BugFix Update	CentOS 7.x x64	CentOS 7.0	Bug Fix	Unspecified		27-Feb-2021		2		Not Approved
CEBA-2021:0623 CentOS 7 microcode_ctl BugFix Update	CentOS 7.x x64	CentOS 7.0	Bug Fix	Unspecified		27-Feb-2021		2		Not Approved
Firefox 86.0 for x64	Windows x64	Firefox	Updates	Unspecified		24-Feb-2021		9		Not Approved
Firefox 86.0 for x86	Windows x32	Firefox	Updates	Unspecified		24-Feb-2021		9		Not Approved
Google Chrome 88.0.4324.190 for x64	Windows x64	Chrome	Updates	Unspecified		24-Feb-2021		9		Not Approved
Zoom 5.5.2	Windows	Zoom	Updates	Unspecified		24-Feb-2021		9		Not Approved

Page: 1 Items per page: 20 1 - 20 of 834

Step 1: Go to *Patches → Patches Catalog*
Step 2: Filter on the patches you would like to set limitations on. Note: Do not forget to use *More Filters* if needed
Step 3: Select the drop down arrow next to *Saved Filters* and select *Save As* to save the filter
Step 4: Go to *Platform Configuration → Servers*



Welcome **Daniel Haid** (Sign out)

JetPatch

Search

Dashboard | Policy | **Servers** | Library | Activities | Logs & Alerts | Users | Settings

JetPatch

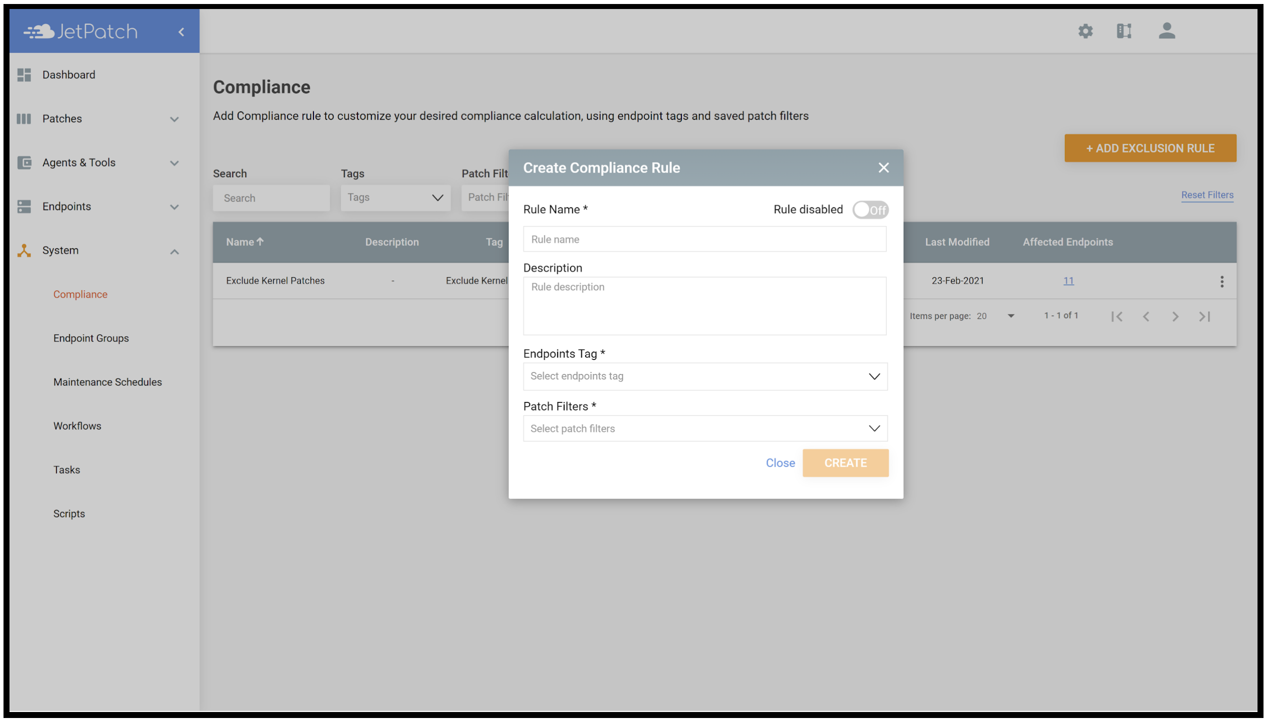
Server Actions · Manage Tags ▾ · Filters (2) ▾ · Manage Smart Groups ▾ · ◀ 1 ▶ · Report ▾ · Table Settings

□	S.	Name	Type	IP	Hostna…	OS	Tags	% C…	Memory I…	Disk Spac…	abt	lert	Int…	In…	Intig	In…	n…	alcc		x…	a…	hro
□		Win…		3.249.1…	EC2AM…	Window…	All Co… × T… ×	100 %	737.91 MiB	20.17 GiB	Z			i			●	●	●	●		
□	⚡	Win…		3.250.8…	ip-0A0A…	Window…	All Co… × T… ×	0 %	560.33 MiB	24.19 GiB				i			●	●	●	●		☒
□	⚡	Win…		52.18.1…	ip-0A00…	Window…	All Co… × T… ×	3 %	1.19 GiB	24.95 GiB					i		●	●	●	●		☒
□	⚡	Win…		34.241.…	EC2AM…	Window…	All Co… × T… ×	0 %	1.64 GiB	15.87 GiB	Z			i			●	●	●	●		
□	⚡	WIN…		34.243.…	WIN-EP-1	Window…	All C… × Wi… ×	0 %	615.56 MiB	23.85 GiB	Z				i			●	●	●		☒
□	⚡	WIN…		63.33.2…	WIN-EP-2	Window…	All C… × Wi… ×	7 %	857.36 MiB	23.62 GiB	Z				i		●	●	●	●		☒
□	⚡	WIN…		34.241.…	WIN-EP-3	Window…	All C… × Wi… ×	2 %	821.56 MiB	24.33 GiB	Z				i		●	●	●	●		☒
□	⚡	WIN…		52.213.…	WIN-EP-4	Window…	All C… × Wi… ×	4 %	829.64 MiB	25.18 GiB	Z				i		●	●	●	●		☒

Recent Activity · Open +

Powered by Intigua © 2020, version 4.1.1.59

Step 5: Select the drop down arrow next to *Manage Tags*, select *New Tag*, and add a new tag
Step 6: Assign the tag to endpoints of the machines you would like to set limitations on by checking the boxes next to the endpoints and selecting *Assign Selected* under the drop down menu in *Manage Tags*
Step 7: Go to *JetPatch* → *System* → *Compliance* --



Compliance

Add Compliance rule to customize your desired compliance calculation, using endpoint tags and saved patch filters

Search: Search | Tags: Tags | Patch Filt: Patch Fil

Name ↑	Description	Tag	Last Modified	Affected Endpoints
Exclude Kernel Patches	-	Exclude Kernel	23-Feb-2021	11

Items per page: 20 | 1 - 1 of 1

Create Compliance Rule

Rule Name * — Rule name — Rule disabled: Off

Description — Rule description

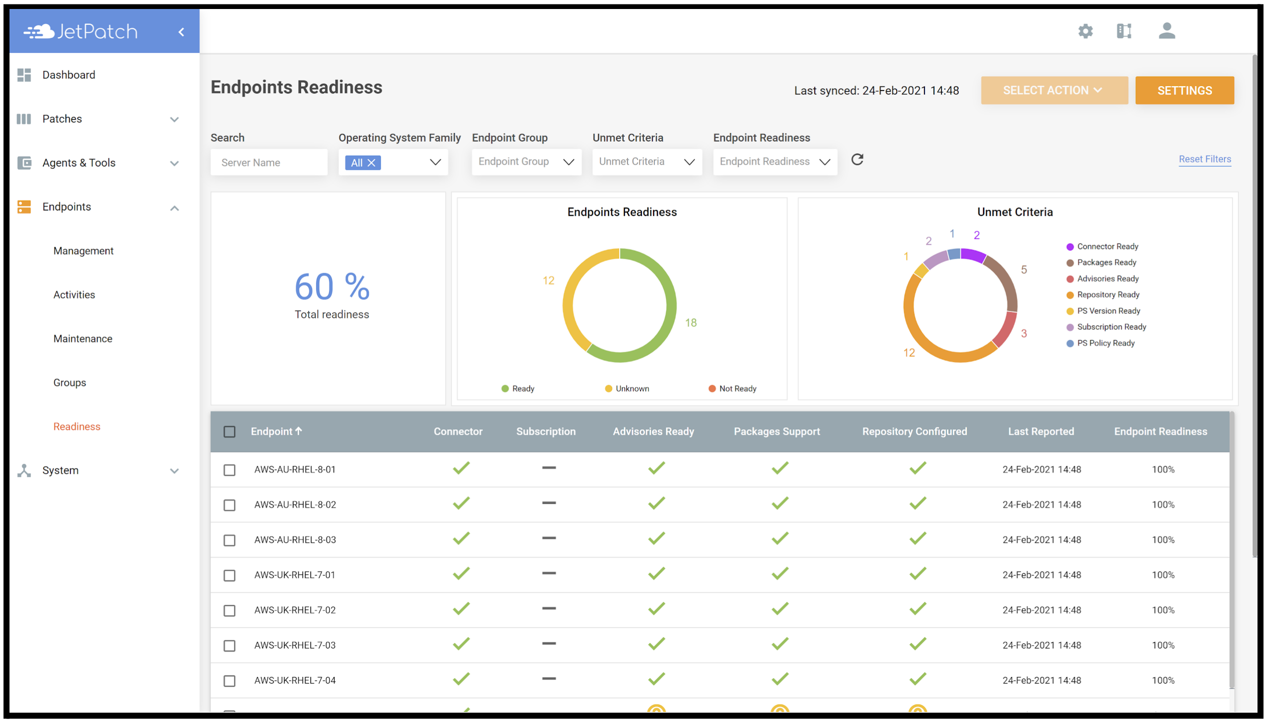
Endpoints Tag * — Select endpoints tag

Patch Filters * — Select patch filters

Step 8: Select + *Add Exclusion Rule*

Step 9: Give *Name*, *Description*, *Endpoints Tag*, and *Saved Filter* created in the process above

Where do I see my Endpoint Compliance versus the Baseline?



Endpoints Readiness

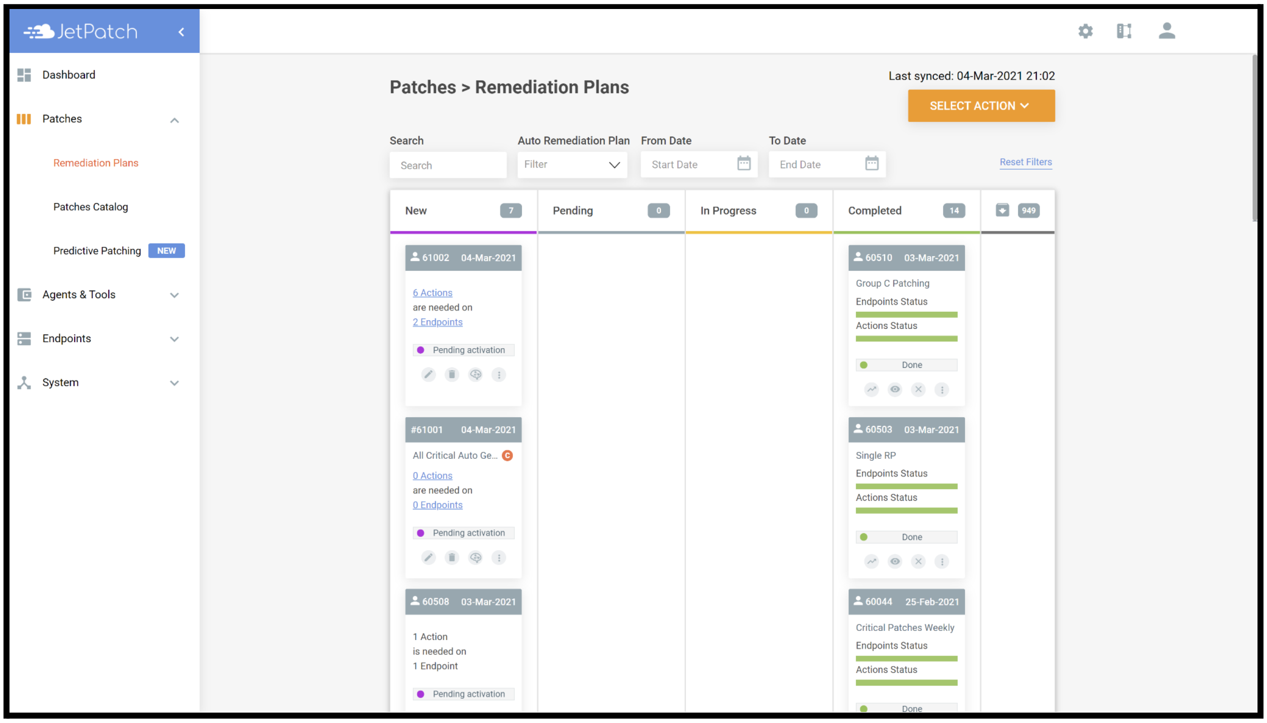
Last synced: 24-Feb-2021 14:48

Search: Server Name
Operating System Family: All
Endpoint Group: Endpoint Group
Unmet Criteria: Unmet Criteria
Endpoint Readiness: Endpoint Readiness

☐	Endpoint ↑	Connector	Subscription	Advisories Ready	Packages Support	Repository Configured	Last Reported	Endpoint Readiness
☐	AWS-AU-RHEL-8-01	✓	—	✓	✓	✓	24-Feb-2021 14:48	100%
☐	AWS-AU-RHEL-8-02	✓	—	✓	✓	✓	24-Feb-2021 14:48	100%
☐	AWS-AU-RHEL-8-03	✓	—	✓	✓	✓	24-Feb-2021 14:48	100%
☐	AWS-UK-RHEL-7-01	✓	—	✓	✓	✓	24-Feb-2021 14:48	100%
☐	AWS-UK-RHEL-7-02	✓	—	✓	✓	✓	24-Feb-2021 14:48	100%
☐	AWS-UK-RHEL-7-03	✓	—	✓	✓	✓	24-Feb-2021 14:48	100%
☐	AWS-UK-RHEL-7-04	✓	—	✓	✓	✓	24-Feb-2021 14:48	100%

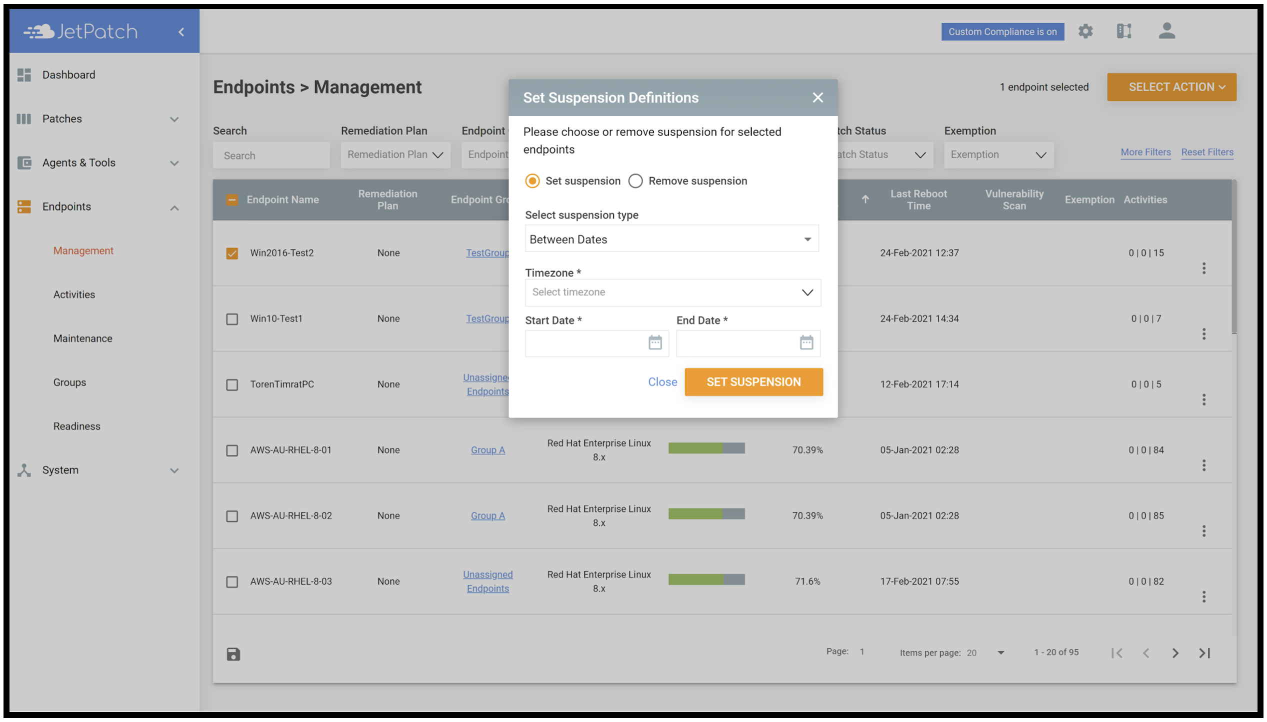
Step 1: Go to *Endpoints → Readiness*
Step 2: Check to see your overall endpoint readiness in the diagrams
Step 3: Narrow down on problematic machines by using filters and sorting columns

I added a New endpoint to a Group. How do I make sure the Endpoint deploys all patches already Approved for the Group?



Step 1: When commissioning a new machine and adding the machine to a group, the endpoint will then install all relevant patches approved previously for that group. If the remediation plans have been deleted, this does not apply and a new remediation plan will need to be created for the previously installed patches.

How do I Exclude specific Endpoints from my Patching Cycle?



Endpoints > Management

1 endpoint selected

Search: Search | Remediation Plan: Remediation Plan | Endpoint: Endpoint | tch Status: atch Status | Exemption: Exemption

Set Suspension Definitions

Please choose or remove suspension for selected endpoints

● Set suspension ○ Remove suspension

Select suspension type: Between Dates

Timezone *: Select timezone

Start Date *

End Date *

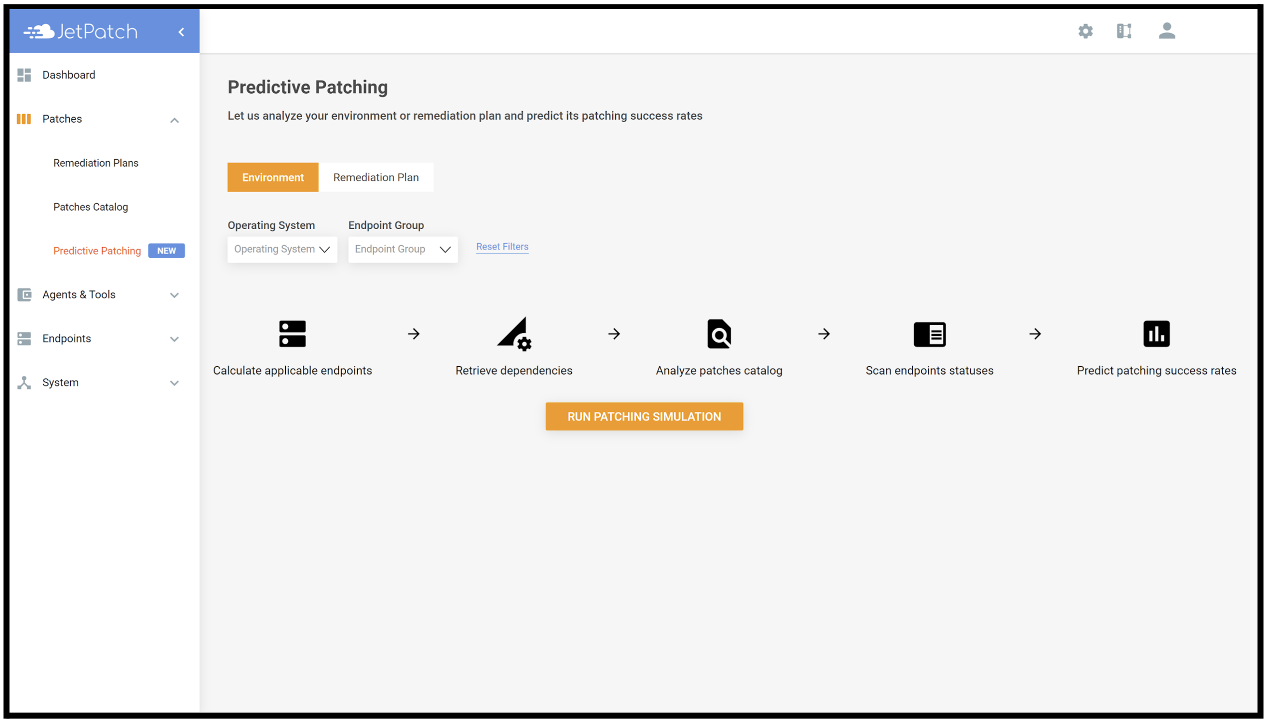
	Endpoint Name	Remediation Plan	Endpoint Gr			↑	Last Reboot Time	Vulnerability Scan	Exemption	Activities
☑	Win2016-Test2	None	TestGroup				24-Feb-2021 12:37			0 | 0 | 15
☐	Win10-Test1	None	TestGroup				24-Feb-2021 14:34			0 | 0 | 7
☐	TorenTimratPC	None	Unassigned Endpoints				12-Feb-2021 17:14			0 | 0 | 5
☐	AWS-AU-RHEL-8-01	None	Group A	Red Hat Enterprise Linux 8.x	🟩	70.39%	05-Jan-2021 02:28			0 | 0 | 84
☐	AWS-AU-RHEL-8-02	None	Group A	Red Hat Enterprise Linux 8.x	🟩	70.39%	05-Jan-2021 02:28			0 | 0 | 85
☐	AWS-AU-RHEL-8-03	None	Unassigned Endpoints	Red Hat Enterprise Linux 8.x	🟩	71.6%	17-Feb-2021 07:55			0 | 0 | 82

Page: 1 Items per page: 20 1 - 20 of 95

Step 1: Go to *Endpoints → Management*
Step 2: Check the endpoint or endpoints you would like to exclude, click *Select Action*, click *Set Suspension*
Step 3: Fill in necessary details. Note: Suspensions can be set by time or maintenance schedules

Predictive Patching

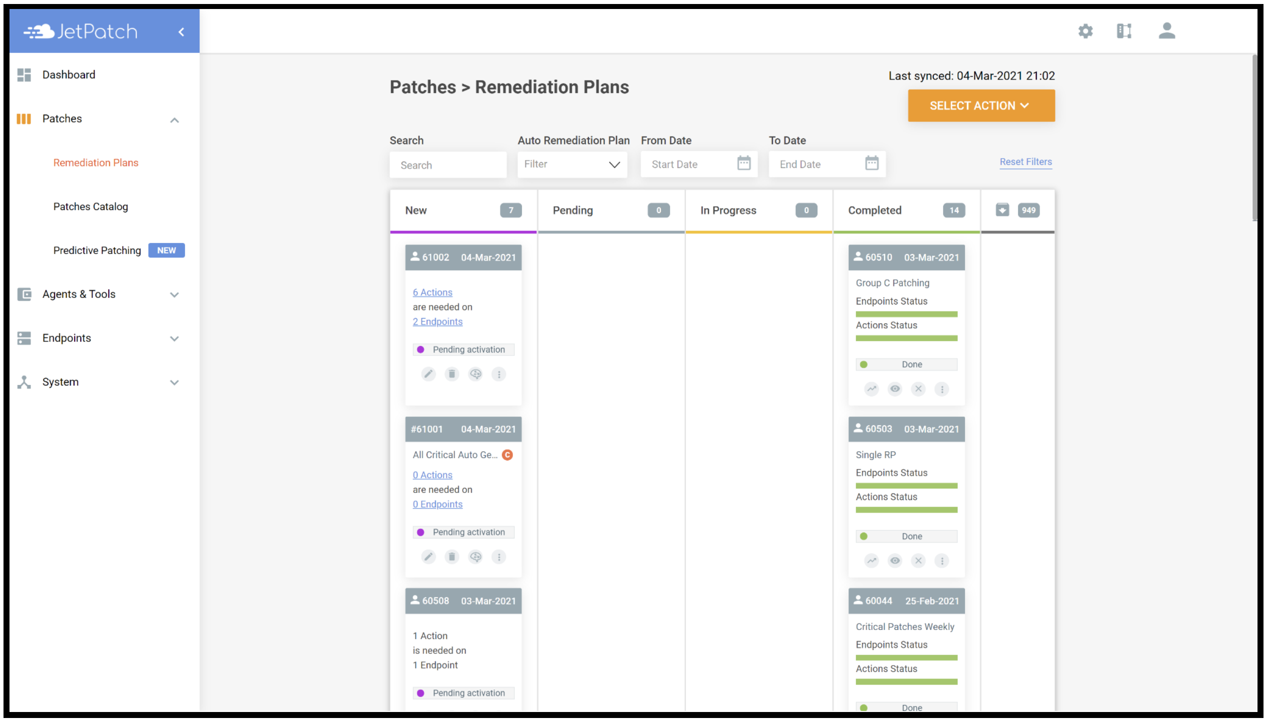
How do I know my Patching Success Rate in my Upcoming Remediation Cycle?



Predictive Patching

Let us analyze your environment or remediation plan and predict its patching success rates

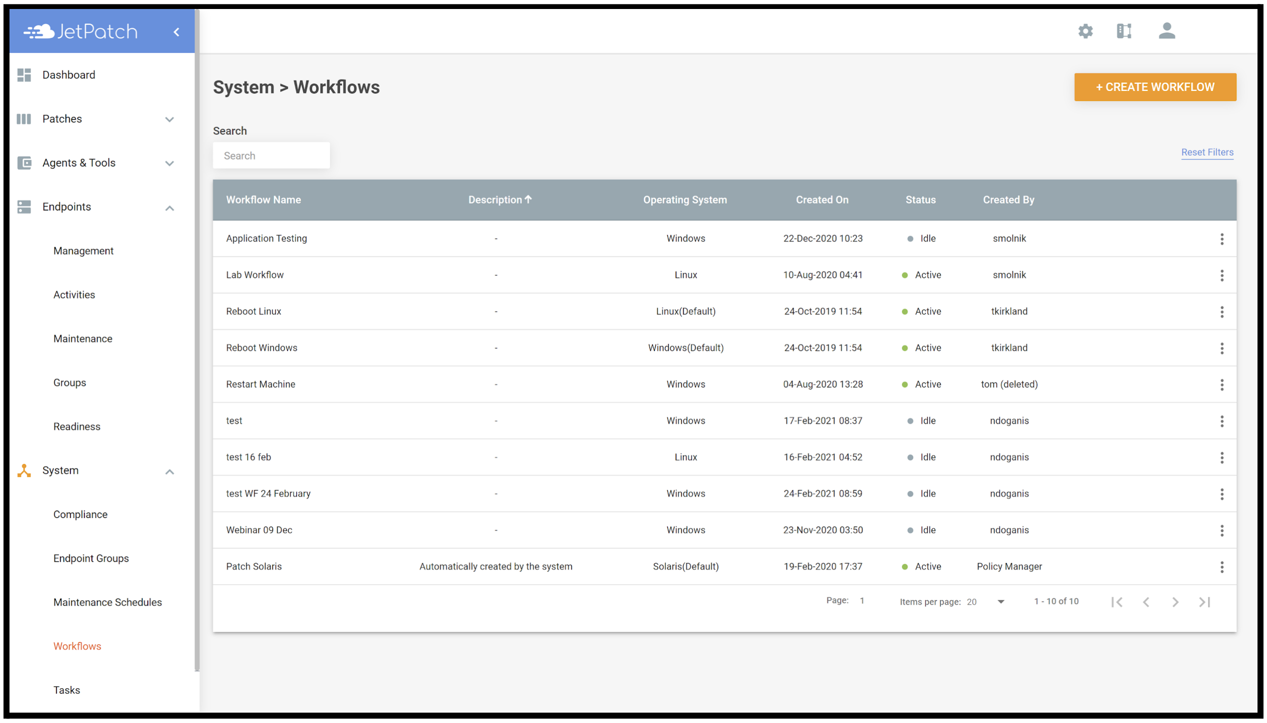
Step 1: Go to *Patches* → *Predictive Patching*
Step 2: Select *Environment* and *Run Patching Simulation* to see the success rate of your entire environment. Note: If the Predicted patching success rate is below 100%, click *How to Improve* to see what endpoints are not in compliance and the reasons why
Step 3: If you are not running your entire environment in the upcoming remediation cycle, you can filter down more closely on, *Operating System*, *Endpoint Group* or *Remediation Plan*



Step 4: If you would like to use predictive patching through the remediation plans dashboard and on a specific plan, go to *Patches → Remediation Plans* and select the *Brain Icon* on the remediation plan

Intelligent Workflow (Pre and Post Patching)

How do I add specific Tasks to be Executed Automatically before and after Patching?



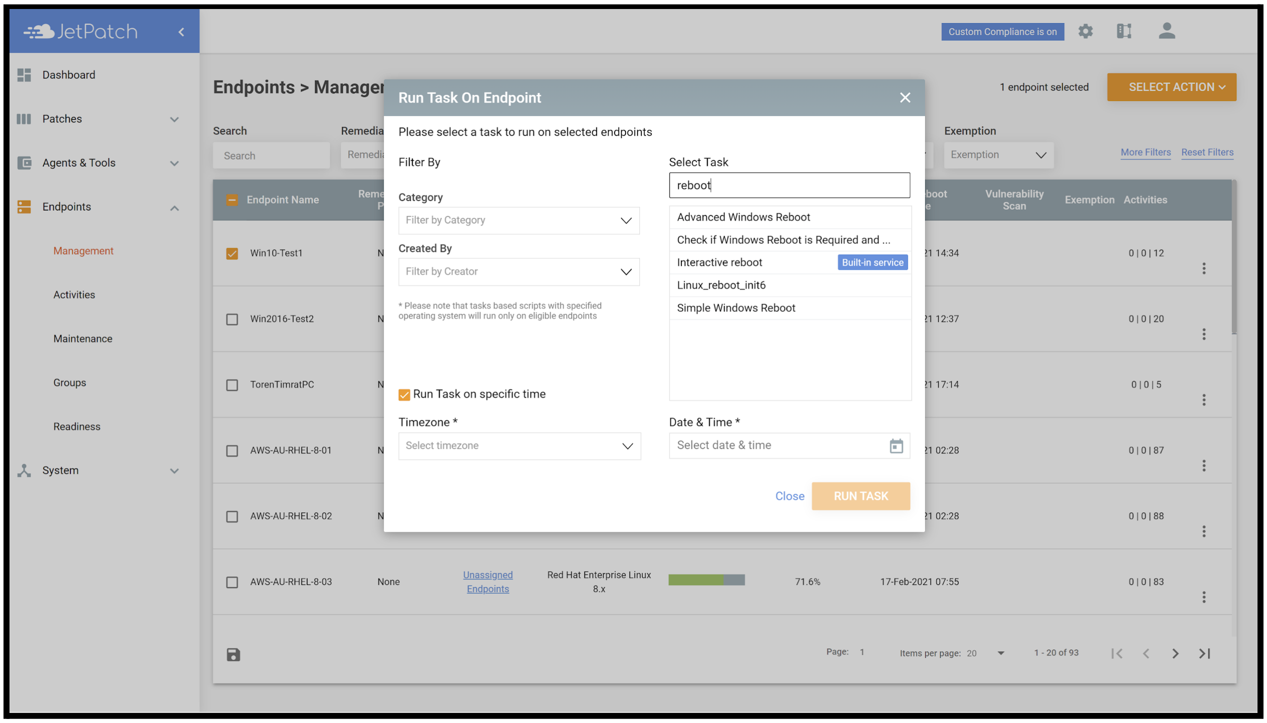
System > Workflows

Workflow Name	Description ↑	Operating System	Created On	Status	Created By
Application Testing	-	Windows	22-Dec-2020 10:23	● Idle	smolnik
Lab Workflow	-	Linux	10-Aug-2020 04:41	● Active	smolnik
Reboot Linux	-	Linux(Default)	24-Oct-2019 11:54	● Active	tkirkland
Reboot Windows	-	Windows(Default)	24-Oct-2019 11:54	● Active	tkirkland
Restart Machine	-	Windows	04-Aug-2020 13:28	● Active	tom (deleted)
test	-	Windows	17-Feb-2021 08:37	● Idle	ndoganis
test 16 feb	-	Linux	16-Feb-2021 04:52	● Idle	ndoganis
test WF 24 February	-	Windows	24-Feb-2021 08:59	● Idle	ndoganis
Webinar 09 Dec	-	Windows	23-Nov-2020 03:50	● Idle	ndoganis
Patch Solaris	Automatically created by the system	Solaris(Default)	19-Feb-2020 17:37	● Active	Policy Manager

Page: 1 Items per page: 20 1 - 10 of 10

Step 1: Go to *Systems* → *Workflows*
Step 2: Create a workflow by selecting + *Create Workflow* and fill in *Name* and *OS*
Step 3: Add a *Built-In* reboot task to *Post-Patching*
Step 4: Use the workflow when manually or automatically creating a remediation plan

How do I Restart my Systems Automatically or at a Specific Time?



Endpoint Name							Activities
☑ Win10-Test1	N					21 14:34	0 | 0 | 12
□ Win2016-Test2	N					21 12:37	0 | 0 | 20
□ TorenTimratPC	N					21 17:14	0 | 0 | 5
□ AWS-AU-RHEL-8-01	N					21 02:28	0 | 0 | 87
□ AWS-AU-RHEL-8-02	N					21 02:28	0 | 0 | 88
□ AWS-AU-RHEL-8-03	None	Unassigned Endpoints	Red Hat Enterprise Linux 8.x		71.6%	17-Feb-2021 07:55	0 | 0 | 83

Run Task On Endpoint

Please select a task to run on selected endpoints

Filter By

Category: Filter by Category

Created By: Filter by Creator

* Please note that tasks based scripts with specified operating system will run only on eligible endpoints

☑ Run Task on specific time

Timezone *: Select timezone

Select Task: reboot

- Advanced Windows Reboot
- Check if Windows Reboot is Required and ...
- Interactive reboot — Built-in service
- Linux_reboot_init6
- Simple Windows Reboot

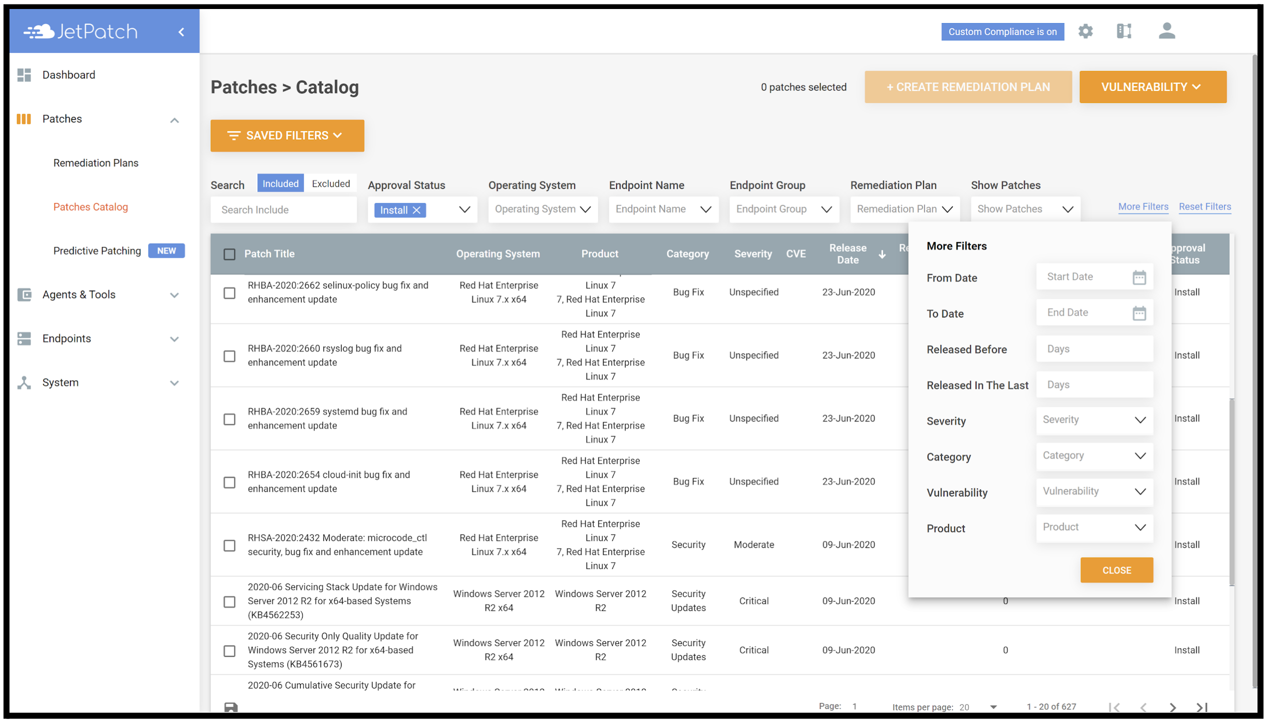
Date & Time *: Select date & time

Close RUN TASK

Step 1: Go to *Endpoints → Management*
Step 2: Select endpoints, click *Select Action* and then *Run Task*
Step 3: Search for reboot task and select it
Step 4: Select *Run Task at Specific Time* for non-immediate execution. Then give *Timezone* and *Date & Time*

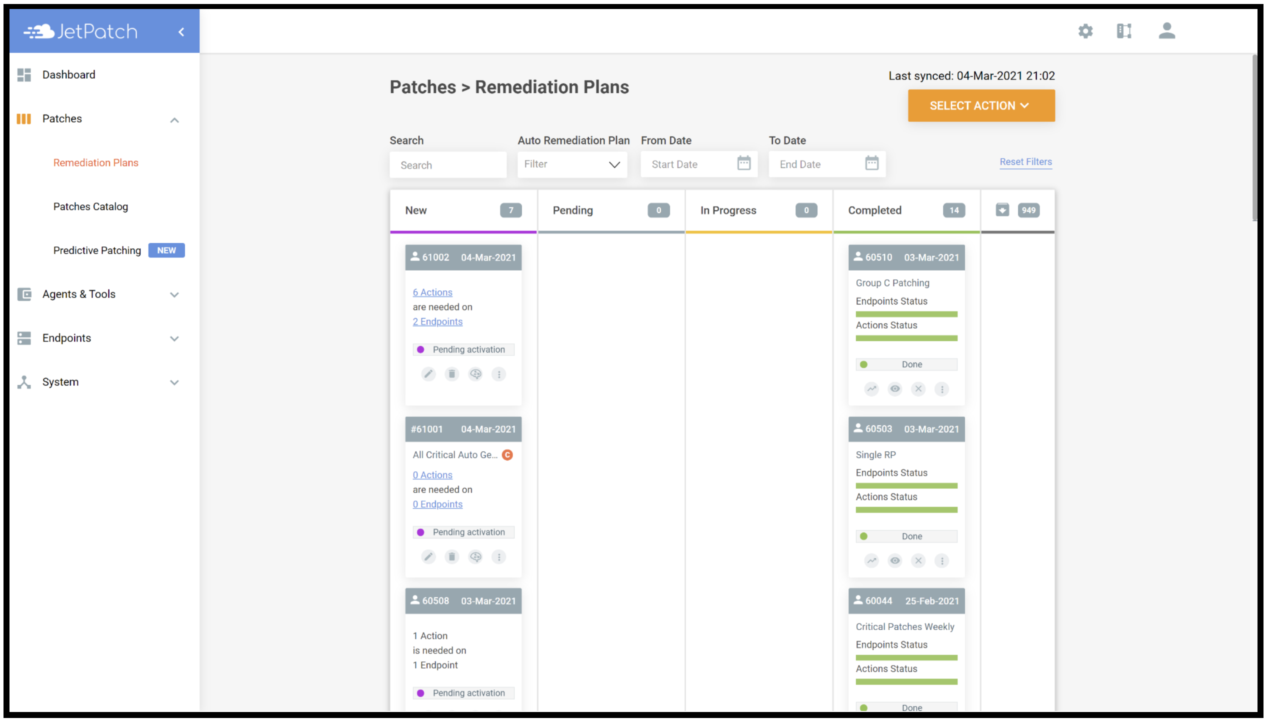
Automatic Remediation

How do I deploy Patches Automatically at a Select Time?



Patch Title	Operating System	Product	Category	Severity	CVE	Release Date	Re		pproval Status
RHBA-2020:2662 selinux-policy bug fix and enhancement update	Red Hat Enterprise Linux 7.x x64	Linux 7 7, Red Hat Enterprise Linux 7	Bug Fix	Unspecified		23-Jun-2020			Install
RHBA-2020:2660 rsyslog bug fix and enhancement update	Red Hat Enterprise Linux 7.x x64	Red Hat Enterprise Linux 7 7, Red Hat Enterprise Linux 7	Bug Fix	Unspecified		23-Jun-2020			Install
RHBA-2020:2659 systemd bug fix and enhancement update	Red Hat Enterprise Linux 7.x x64	Red Hat Enterprise Linux 7 7, Red Hat Enterprise Linux 7	Bug Fix	Unspecified		23-Jun-2020			Install
RHBA-2020:2654 cloud-init bug fix and enhancement update	Red Hat Enterprise Linux 7.x x64	Red Hat Enterprise Linux 7 7, Red Hat Enterprise Linux 7	Bug Fix	Unspecified		23-Jun-2020			Install
RHSA-2020:2432 Moderate: microcode_ctl security, bug fix and enhancement update	Red Hat Enterprise Linux 7.x x64	Red Hat Enterprise Linux 7 7, Red Hat Enterprise Linux 7	Security	Moderate		09-Jun-2020			Install
2020-06 Servicing Stack Update for Windows Server 2012 R2 for x64-based Systems (KB4562253)	Windows Server 2012 R2 x64	Windows Server 2012 R2	Security Updates	Critical		09-Jun-2020		0	Install
2020-06 Security Only Quality Update for Windows Server 2012 R2 for x64-based Systems (KB4561673)	Windows Server 2012 R2 x64	Windows Server 2012 R2	Security Updates	Critical		09-Jun-2020		0	Install
2020-06 Cumulative Security Update for									

Step 1: Go to *Patches → Patches Catalog*
Step 2: Filter to the type of patches you are looking for. Do not forget you can use *More Filters*
Step 3: Click on *Saved Filters*, click *Save As* and fill in the *Name* and *Description*. Click *Save*
Step 4: Go to *Patches → Remediation Plans*



Patches > Remediation Plans

Last synced: 04-Mar-2021 21:02

Search: Search
Auto Remediation Plan: Filter
From Date: Start Date
To Date: End Date

New 7 | Pending 0 | In Progress 0 | Completed 14 | 949

61002 04-Mar-2021
6 Actions are needed on 2 Endpoints
Pending activation

#61001 04-Mar-2021
All Critical Auto Ge... C
0 Actions are needed on 0 Endpoints
Pending activation

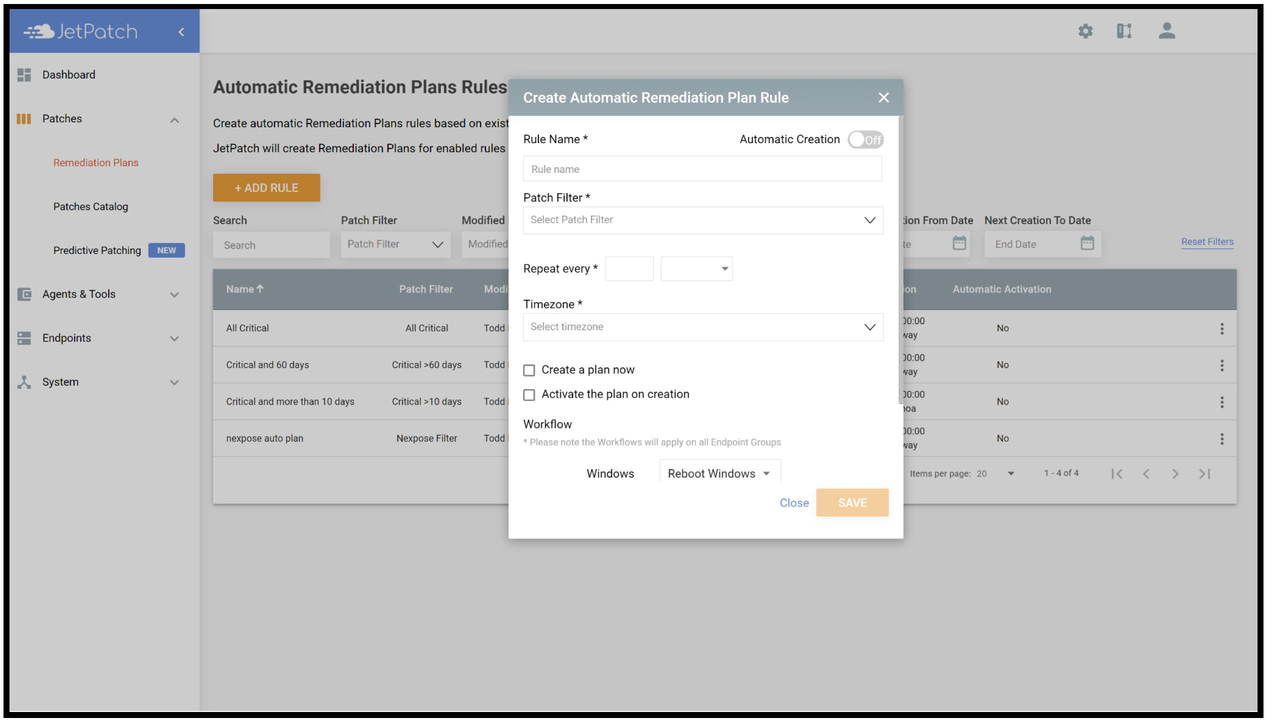
60508 03-Mar-2021
1 Action is needed on 1 Endpoint
Pending activation

60510 03-Mar-2021
Group C Patching
Endpoints Status
Actions Status
Done

60503 03-Mar-2021
Single RP
Endpoints Status
Actions Status
Done

60044 25-Feb-2021
Critical Patches Weekly
Endpoints Status
Actions Status
Done

Step 5: *Select Action → Create/Edit Remediation Plan Rules*



Automatic Remediation Plans Rules

Create automatic Remediation Plans rules based on exist…

JetPatch will create Remediation Plans for enabled rules…

Name	Patch Filter	Modi…	…on	Automatic Activation
All Critical	All Critical	Todd…	…00:00 …way	No
Critical and 60 days	Critical >60 days	Todd…	…00:00 …way	No
Critical and more than 10 days	Critical >10 days	Todd…	…00:00 …oa	No
nexpose auto plan	Nexpose Filter	Todd…	…00:00 …way	No

Create Automatic Remediation Plan Rule

Rule Name * Automatic Creation Off

Rule name

Patch Filter *

Select Patch Filter

Repeat every *

Timezone *

Select timezone

☐ Create a plan now

☐ Activate the plan on creation

Workflow

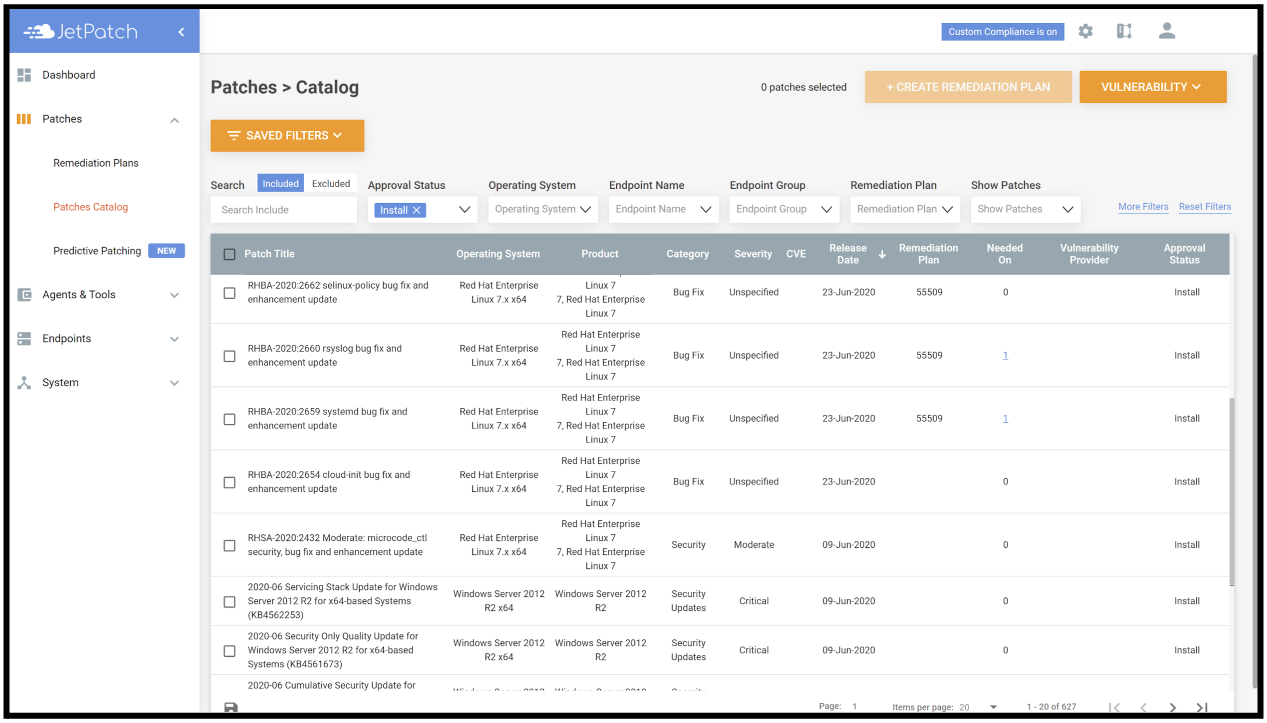
* Please note the Workflows will apply on all Endpoint Groups

Windows Reboot Windows

Step 6: Click *+ Add Rule*
Step 7: Give *Name*, *Patch Filter* created above, how often you would like the plan to repeat, *Time Zone*
Step 8: Selecting *Create a Plan Now* will automatically create a plan once saved
Step 9: Selecting *Activate the Plan on Creation* will move the plan from the *New* column to the *Pending* column automatically
Step 10: Select the workflow(s) you would like to use for the remediation plan
Step 11: Select *Save* and enable *Automatic Creation* at the top right of the window

Selective Remediation

How do I Deploy Individual and/or Group Patches?



Patches > Catalog

0 patches selected

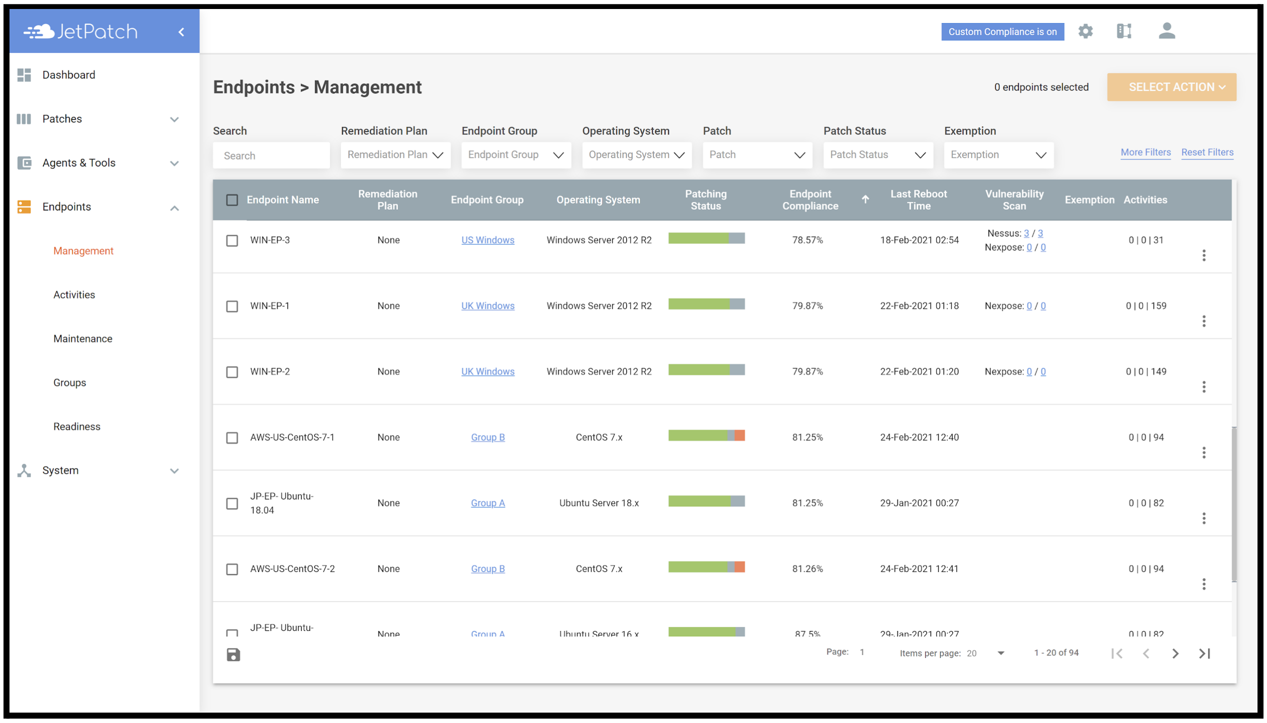
Search: Included | Excluded — Search Include
Approval Status: Install
Operating System: Operating System
Endpoint Name: Endpoint Name
Endpoint Group: Endpoint Group
Remediation Plan: Remediation Plan
Show Patches: Show Patches

□	Patch Title	Operating System	Product	Category	Severity	CVE	Release Date ↓	Remediation Plan	Needed On	Vulnerability Provider	Approval Status
□	RHBA-2020:2662 selinux-policy bug fix and enhancement update	Red Hat Enterprise Linux 7.x x64	Linux 7 7, Red Hat Enterprise Linux 7	Bug Fix	Unspecified		23-Jun-2020	55509	0		Install
□	RHBA-2020:2660 rsyslog bug fix and enhancement update	Red Hat Enterprise Linux 7.x x64	Red Hat Enterprise Linux 7 7, Red Hat Enterprise Linux 7	Bug Fix	Unspecified		23-Jun-2020	55509	1		Install
□	RHBA-2020:2659 systemd bug fix and enhancement update	Red Hat Enterprise Linux 7.x x64	Red Hat Enterprise Linux 7 7, Red Hat Enterprise Linux 7	Bug Fix	Unspecified		23-Jun-2020	55509	1		Install
□	RHBA-2020:2654 cloud-init bug fix and enhancement update	Red Hat Enterprise Linux 7.x x64	Red Hat Enterprise Linux 7 7, Red Hat Enterprise Linux 7	Bug Fix	Unspecified		23-Jun-2020		0		Install
□	RHSA-2020:2432 Moderate: microcode_ctl security, bug fix and enhancement update	Red Hat Enterprise Linux 7.x x64	Red Hat Enterprise Linux 7 7, Red Hat Enterprise Linux 7	Security	Moderate		09-Jun-2020		0		Install
□	2020-06 Servicing Stack Update for Windows Server 2012 R2 for x64-based Systems (KB4562253)	Windows Server 2012 R2 x64	Windows Server 2012 R2	Security Updates	Critical		09-Jun-2020		0		Install
□	2020-06 Security Only Quality Update for Windows Server 2012 R2 for x64-based Systems (KB4561673)	Windows Server 2012 R2 x64	Windows Server 2012 R2	Security Updates	Critical		09-Jun-2020		0		Install
	2020-06 Cumulative Security Update for										

Page: 1   Items per page: 20   1 - 20 of 627

Step 1: Go to *Patches → Patches Catalog*
Step 2: Filter through the patches to find which patch(es) you are looking for. Note: Do not forget to sort through the *More Filter*s Section
Step 3: Select the patch(es) by clicking the empty box to the left of the specific patch(es) title. Note: Select the grey box to select all patches filtered
Step 4: Select + *Create Remediation Plan*
Step 5: Configure Plan: Give a *Name*, *Description* and select the *SLA Start and End* date. Click *Save and Continue*
Step 6: Approve Plan: Select the patch(es) by clicking the empty box to the left of *Patch Title*. Select the drop down arrow next to *Select Bulk Action* and click *Bulk Install* to install all patches. Click *Save and Continue*
Step 7: Create Cycle: Select the group(s) and workflow(s) for the plan. Click *Save Cycle* to save the plan details in the *New* column of your *Remediation Plans* dashboard. Click *Save & Activate Plan* to automatically move the plan into the *Pending* column to start the remediation process

How to Create a Remediation Plan Based on my Vulnerability Scanner Report?



Endpoints > Management

0 endpoints selected

	Endpoint Name	Remediation Plan	Endpoint Group	Operating System	Patching Status	Endpoint Compliance	Last Reboot Time	Vulnerability Scan	Exemption	Activities
□	WIN-EP-3	None	US Windows	Windows Server 2012 R2		78.57%	18-Feb-2021 02:54	Nessus: 3 / 3 Nexpose: 0 / 0		0 | 0 | 31
□	WIN-EP-1	None	UK Windows	Windows Server 2012 R2		79.87%	22-Feb-2021 01:18	Nexpose: 0 / 0		0 | 0 | 159
□	WIN-EP-2	None	UK Windows	Windows Server 2012 R2		79.87%	22-Feb-2021 01:20	Nexpose: 0 / 0		0 | 0 | 149
□	AWS-US-CentOS-7-1	None	Group B	CentOS 7.x		81.25%	24-Feb-2021 12:40			0 | 0 | 94
□	JP-EP- Ubuntu-18.04	None	Group A	Ubuntu Server 18.x		81.25%	29-Jan-2021 00:27			0 | 0 | 82
□	AWS-US-CentOS-7-2	None	Group B	CentOS 7.x		81.26%	24-Feb-2021 12:41			0 | 0 | 94
□	JP-EP- Ubuntu-	None	Group A	Ubuntu Server 16.x		87.5%	29-Jan-2021 00:27			0 | 0 | 82

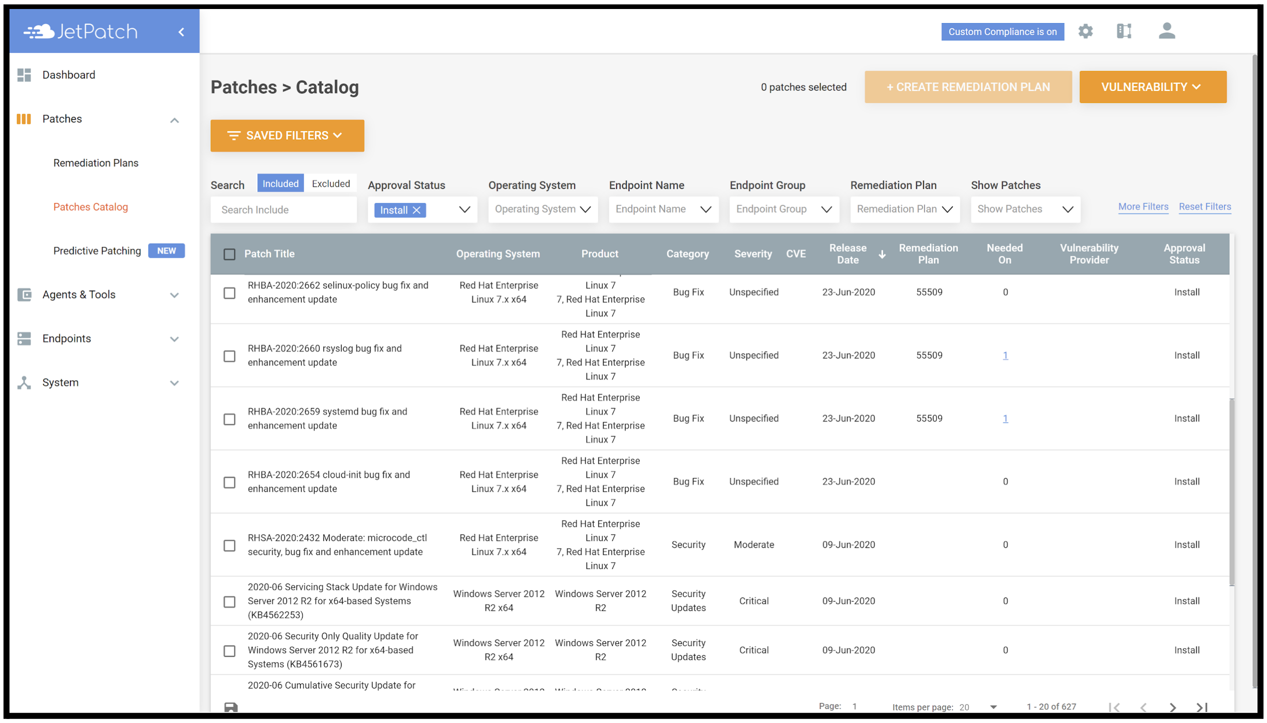
Page: 1 Items per page: 20 1 - 20 of 94

Step 1: Go to *Endpoints → Management*
Step 2: Use relevant filters to sort on endpoints to remediate
Step 2: Select endpoints by checking the box(es) to the left hand side. Note: Checking the grey box will select all
Step 3: Click *Select Action* and then *Create a Remediation Plan Based On* the specific vulnerability scanner
Step 4: Select *Edit Plan* at the bottom to start the activation process (this will show up after step 3 has been completed)
Step 5: Configure Plan: Give a *Name*, *Description* and select the *SLA Start and End* date. Click *Save and Continue*
Step 6: Approve Plan: Select the patch(es) by clicking the empty box to the left of *Patch Title*. Select the drop down arrow next to *Select Bulk Action* and click *Bulk Install* to install all patches. Click *Save and Continue*
Step 7: Create Cycle: Select the group(s) and workflow(s) for the plan. Click *Save Cycle* to save the plan details in the *New* column of your *Remediation Plans* dashboard. Click *Save & Activate Plan* to automatically move the plan into the *Pending* column to start the remediation process

How do I Rollback Patches or a Completed Remediation Plan?

Note: Rolling back is only applicable for enabled patch(es)

Option 1: Patches



Patches > Catalog

0 patches selected

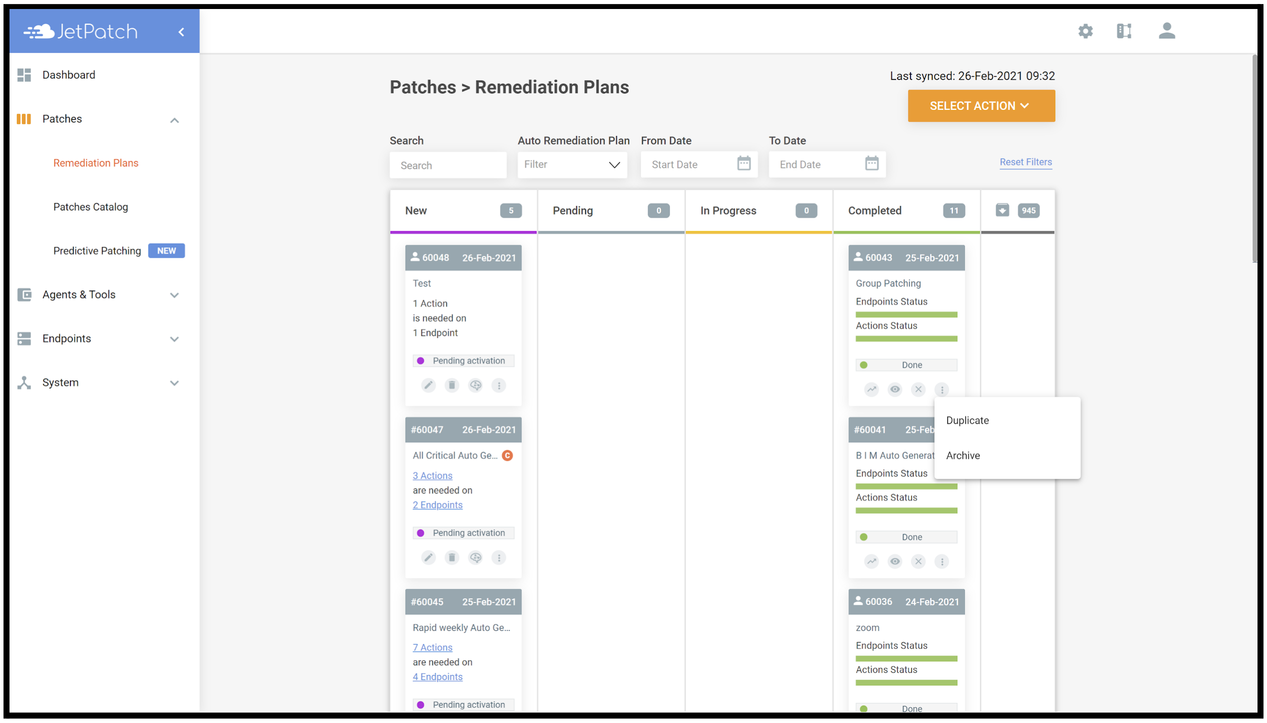
Search: Included | Excluded — Search Include
Approval Status: Install
Operating System: Operating System
Endpoint Name: Endpoint Name
Endpoint Group: Endpoint Group
Remediation Plan: Remediation Plan
Show Patches: Show Patches

□ Patch Title	Operating System	Product	Category	Severity	CVE	Release Date	Remediation Plan	Needed On	Vulnerability Provider	Approval Status
□ RHBA-2020:2662 selinux-policy bug fix and enhancement update	Red Hat Enterprise Linux 7.x x64	Linux 7 7, Red Hat Enterprise Linux 7	Bug Fix	Unspecified		23-Jun-2020	55509	0		Install
□ RHBA-2020:2660 rsyslog bug fix and enhancement update	Red Hat Enterprise Linux 7.x x64	Red Hat Enterprise Linux 7 7, Red Hat Enterprise Linux 7	Bug Fix	Unspecified		23-Jun-2020	55509	1		Install
□ RHBA-2020:2659 systemd bug fix and enhancement update	Red Hat Enterprise Linux 7.x x64	Red Hat Enterprise Linux 7 7, Red Hat Enterprise Linux 7	Bug Fix	Unspecified		23-Jun-2020	55509	1		Install
□ RHBA-2020:2654 cloud-init bug fix and enhancement update	Red Hat Enterprise Linux 7.x x64	Red Hat Enterprise Linux 7 7, Red Hat Enterprise Linux 7	Bug Fix	Unspecified		23-Jun-2020		0		Install
□ RHSA-2020:2432 Moderate: microcode_ctl security, bug fix and enhancement update	Red Hat Enterprise Linux 7.x x64	Red Hat Enterprise Linux 7 7, Red Hat Enterprise Linux 7	Security	Moderate		09-Jun-2020		0		Install
□ 2020-06 Servicing Stack Update for Windows Server 2012 R2 for x64-based Systems (KB4562253)	Windows Server 2012 R2 x64	Windows Server 2012 R2	Security Updates	Critical		09-Jun-2020		0		Install
□ 2020-06 Security Only Quality Update for Windows Server 2012 R2 for x64-based Systems (KB4561673)	Windows Server 2012 R2 x64	Windows Server 2012 R2	Security Updates	Critical		09-Jun-2020		0		Install
2020-06 Cumulative Security Update for										

Page: 1 Items per page: 20 1 - 20 of 627

Step 1: Go to *Patches → Patches Catalog*
Step 2: Filter on patch(es) you would like to rollback
Step 3: Select + *Create Remediation Plan*
Step 4: Configure Plan: Give a *Name*, *Description* and select the *SLA Start and End* date. Click *Save and Continue*
Step 5: Approve Plan: Select the patch(es) by clicking the empty box to the left of *Patch Title*. Select the drop down arrow next to *Select Bulk Action* and click *Bulk Remove* to rollback all patches. Click *Save and Continue*
Step 6: Create Cycle: Select the group(s) and workflow(s) for the plan. Click *Save Cycle* to save the plan details in the *New* column of your *Remediation Plans* dashboard. Click *Save & Activate Plan* to automatically move the plan into the *Pending* column to start the remediation process

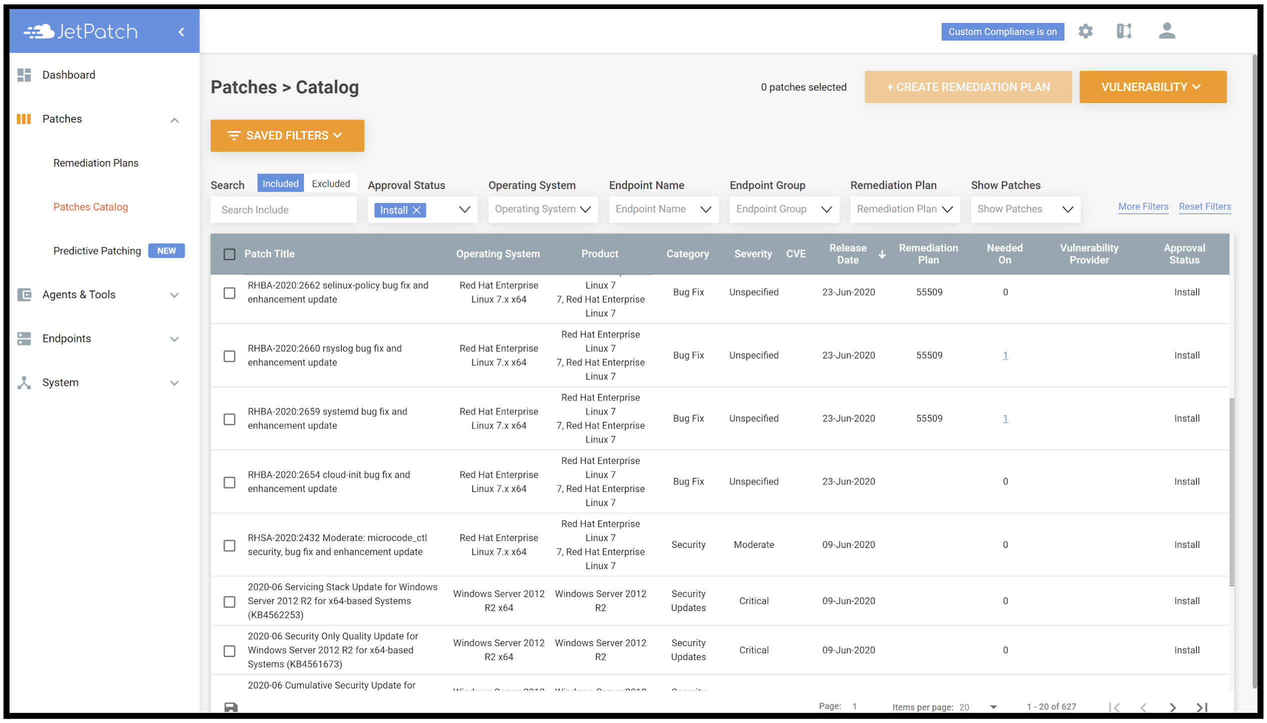
Option 2: Remediation Plans



Step 1: Go to *Patches → Remediation Plans*
Step 2: Find the remediation plan you would like to rollback, select the 3 dots icon, and click duplicate
Step 3: Find the duplicate plan in the *New* column and select edit
Step 4: Configure Plan: Give a *Name*, *Description* and select the *SLA Start and End* date. Click *Save and Continue*
Step 5: Approve Plan: Select the patch(es) by clicking the empty box to the left of *Patch Title*. Select the drop down arrow next to *Select Bulk Action* and click *Bulk Remove* to rollback all patches. Click *Save and Continue*
Step 6: Create Cycle: Select the group(s) and workflow(s) for the plan. Click *Save Cycle* to save the plan details in the *New* column of your *Remediation Plans* dashboard. Click *Save & Activate Plan* to automatically move the plan into the *Pending* column to start the remediation process

Emergency Remediation

How do I Deploy an Emergency Patch in my Environment (Zero-day Patch)?



Patches > Catalog

0 patches selected

Search: Included | Excluded — Search Include
Approval Status: Install
Operating System: Operating System
Endpoint Name: Endpoint Name
Endpoint Group: Endpoint Group
Remediation Plan: Remediation Plan
Show Patches: Show Patches

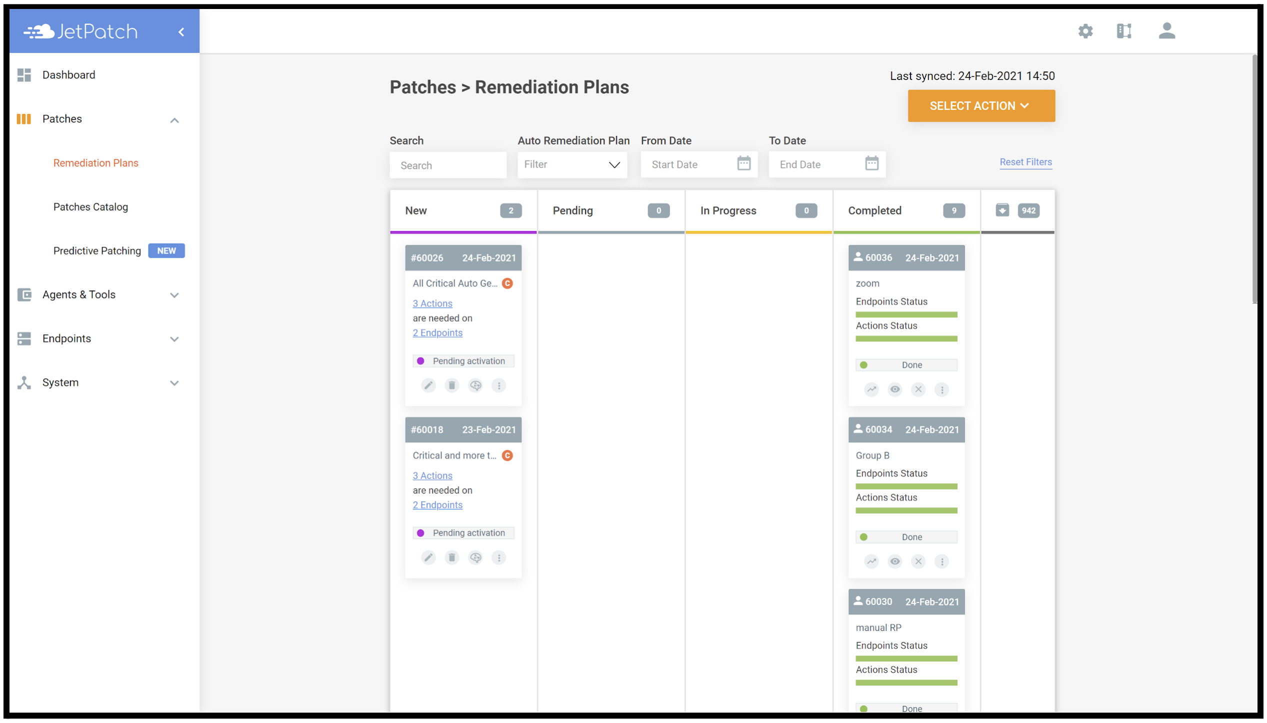
☐ Patch Title	Operating System	Product	Category	Severity	CVE	Release Date	Remediation Plan	Needed On	Vulnerability Provider	Approval Status
☐ RHBA-2020:2662 selinux-policy bug fix and enhancement update	Red Hat Enterprise Linux 7.x x64	Linux 7 7, Red Hat Enterprise Linux 7	Bug Fix	Unspecified		23-Jun-2020	55509	0		Install
☐ RHBA-2020:2660 rsyslog bug fix and enhancement update	Red Hat Enterprise Linux 7.x x64	Red Hat Enterprise Linux 7 7, Red Hat Enterprise Linux 7	Bug Fix	Unspecified		23-Jun-2020	55509	1		Install
☐ RHBA-2020:2659 systemd bug fix and enhancement update	Red Hat Enterprise Linux 7.x x64	Red Hat Enterprise Linux 7 7, Red Hat Enterprise Linux 7	Bug Fix	Unspecified		23-Jun-2020	55509	1		Install
☐ RHBA-2020:2654 cloud-init bug fix and enhancement update	Red Hat Enterprise Linux 7.x x64	Red Hat Enterprise Linux 7 7, Red Hat Enterprise Linux 7	Bug Fix	Unspecified		23-Jun-2020		0		Install
☐ RHSA-2020:2432 Moderate: microcode_ctl security, bug fix and enhancement update	Red Hat Enterprise Linux 7.x x64	Red Hat Enterprise Linux 7 7, Red Hat Enterprise Linux 7	Security	Moderate		09-Jun-2020		0		Install
☐ 2020-06 Servicing Stack Update for Windows Server 2012 R2 for x64-based Systems (KB4562253)	Windows Server 2012 R2 x64	Windows Server 2012 R2	Security Updates	Critical		09-Jun-2020		0		Install
☐ 2020-06 Security Only Quality Update for Windows Server 2012 R2 for x64-based Systems (KB4561673)	Windows Server 2012 R2 x64	Windows Server 2012 R2	Security Updates	Critical		09-Jun-2020		0		Install
2020-06 Cumulative Security Update for										

Page: 1 Items per page: 20 1 - 20 of 627

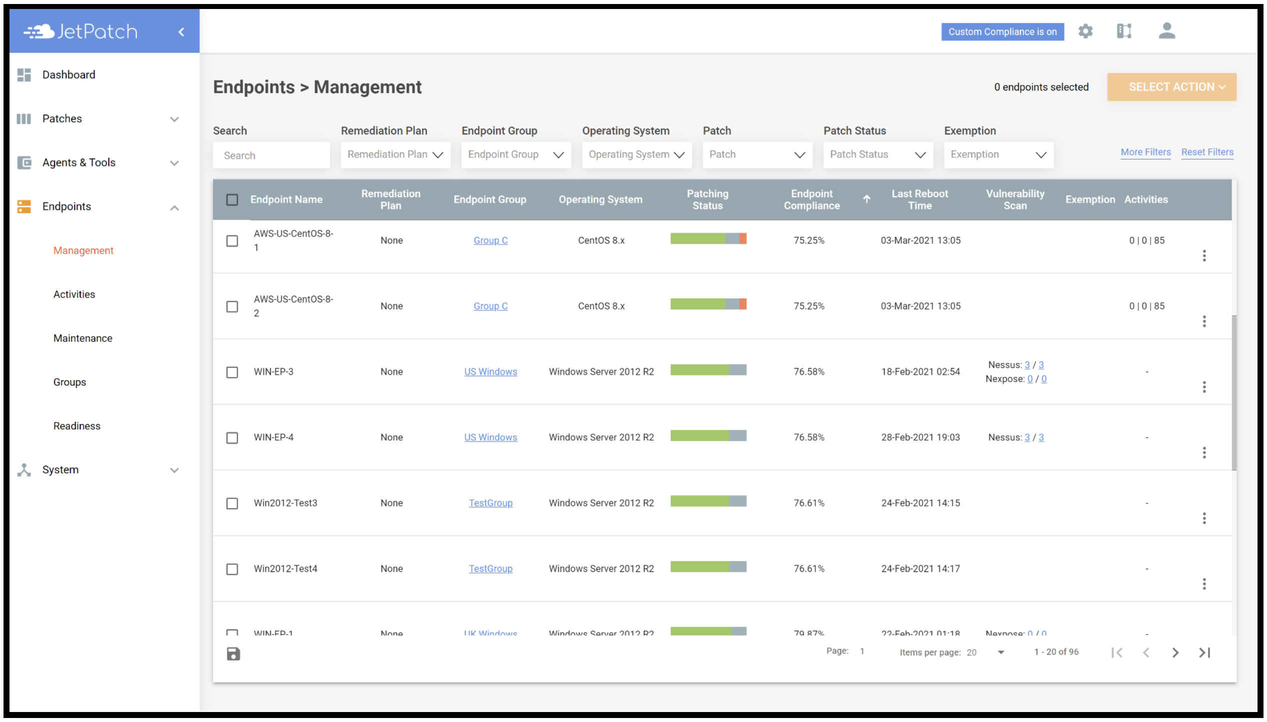
Step 1: Go to *System* → *Patches Catalog*
Step 2: Create a *Remediation Plan*
Step 3: Configure Plan: Give a *Name*, *Description* and select the *SLA Start and End* date. Click *Save and Continue.*
Step 4: Select *Emergency Remediation Plan*. Note: This will override the maintenance schedules for all endpoints involved for this specific remediation plan
Step 5: Approve Plan: Select the patch(es) by clicking the empty box to the left of *Patch Title*. Select the drop down arrow next to *Select Bulk Action* and click *Bulk Remove* to rollback all patches. Click *Save and Continue*
Step 6: Create Cycle: Select the group(s) and workflow(s) for the plan.
Step 7: Select the *Emergency Maintenance Window*
Step 8: Click *Save Cycle* to save the plan details in the *New* column of your *Remediation Plans* dashboard. Click *Save & Activate Plan* to automatically move the plan into the *Pending* column to start the remediation process

Reporting

Reporting the Compliance of my In Progress or Finished Remediation Plans



Step 1: Go to *Patches → Remediations Plans*
Step 2: Go to the specific remediation plan and select *Compliance Report*
Step 3: Scroll down to relevant patches or endpoints to view the breakdown and or patching status. Note: To download the report, follow the remaining steps



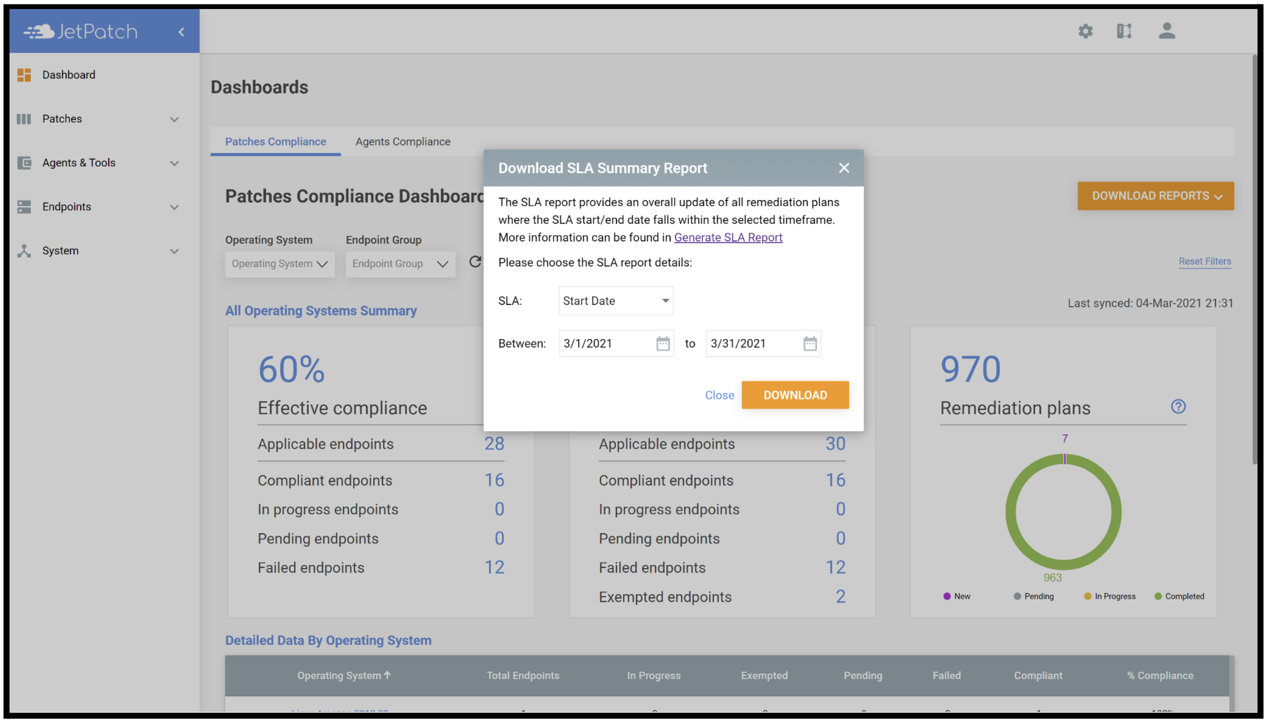
Endpoints > Management

☐	Endpoint Name	Remediation Plan	Endpoint Group	Operating System	Patching Status	Endpoint Compliance ↑	Last Reboot Time	Vulnerability Scan	Exemption	Activities
☐	AWS-US-CentOS-8-1	None	Group C	CentOS 8.x		75.25%	03-Mar-2021 13:05			0 | 0 | 85
☐	AWS-US-CentOS-8-2	None	Group C	CentOS 8.x		75.25%	03-Mar-2021 13:05			0 | 0 | 85
☐	WIN-EP-3	None	US Windows	Windows Server 2012 R2		76.58%	18-Feb-2021 02:54	Nessus: 3 / 3 Nexpose: 0 / 0		-
☐	WIN-EP-4	None	US Windows	Windows Server 2012 R2		76.58%	28-Feb-2021 19:03	Nessus: 3 / 3		-
☐	Win2012-Test3	None	TestGroup	Windows Server 2012 R2		76.61%	24-Feb-2021 14:15			-
☐	Win2012-Test4	None	TestGroup	Windows Server 2012 R2		76.61%	24-Feb-2021 14:17			-
☐	WIN-EP-1	None	UK Windows	Windows Server 2012 R2		79.87%	22-Feb-2021 01:18	Nexpose: 0 / 0		-

Page: 1 Items per page: 20 1 - 20 of 96

Step 4: Go to *Endpoints → Management*
Step 5: Filter on *Remediation Plan* to find your specific plan(s)
Step 6: Select the *Floppy Disc* icon in the bottom right corner, select *Endpoints Management Report* and then select *Download*

Reporting on my Patching SLAs?



Download SLA Summary Report

The SLA report provides an overall update of all remediation plans where the SLA start/end date falls within the selected timeframe. More information can be found in Generate SLA Report

Please choose the SLA report details:

SLA: Start Date

Between: 3/1/2021 to 3/31/2021

Close DOWNLOAD

60%
Effective compliance

Applicable endpoints	28
Compliant endpoints	16
In progress endpoints	0
Pending endpoints	0
Failed endpoints	12

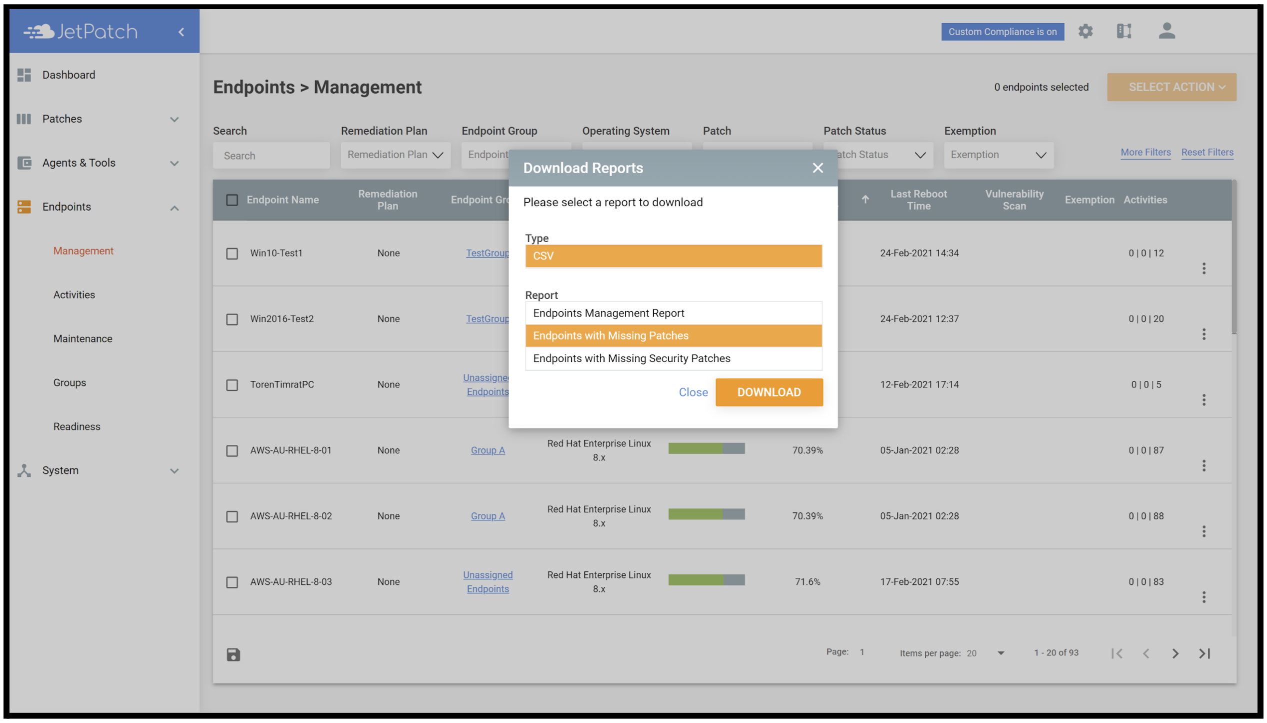
Applicable endpoints	30
Compliant endpoints	16
In progress endpoints	0
Pending endpoints	0
Failed endpoints	12
Exempted endpoints	2

970
Remediation plans

Operating System	Total Endpoints	In Progress	Exempted	Pending	Failed	Compliant	% Compliance

Step 1: Go to *Dashboard*
Step 2: Select *Download Reports* and then click *SLA Summary*
Step 3: Fill in whether you would like the report to be based off the *SLA start or end* date and then give a date range
Step 4: Select *Download*

Reporting on Systems Missing Critical Patches?



Download Reports

Please select a report to download

Type

CSV

Report

- Endpoints Management Report
- Endpoints with Missing Patches
- Endpoints with Missing Security Patches

Close DOWNLOAD

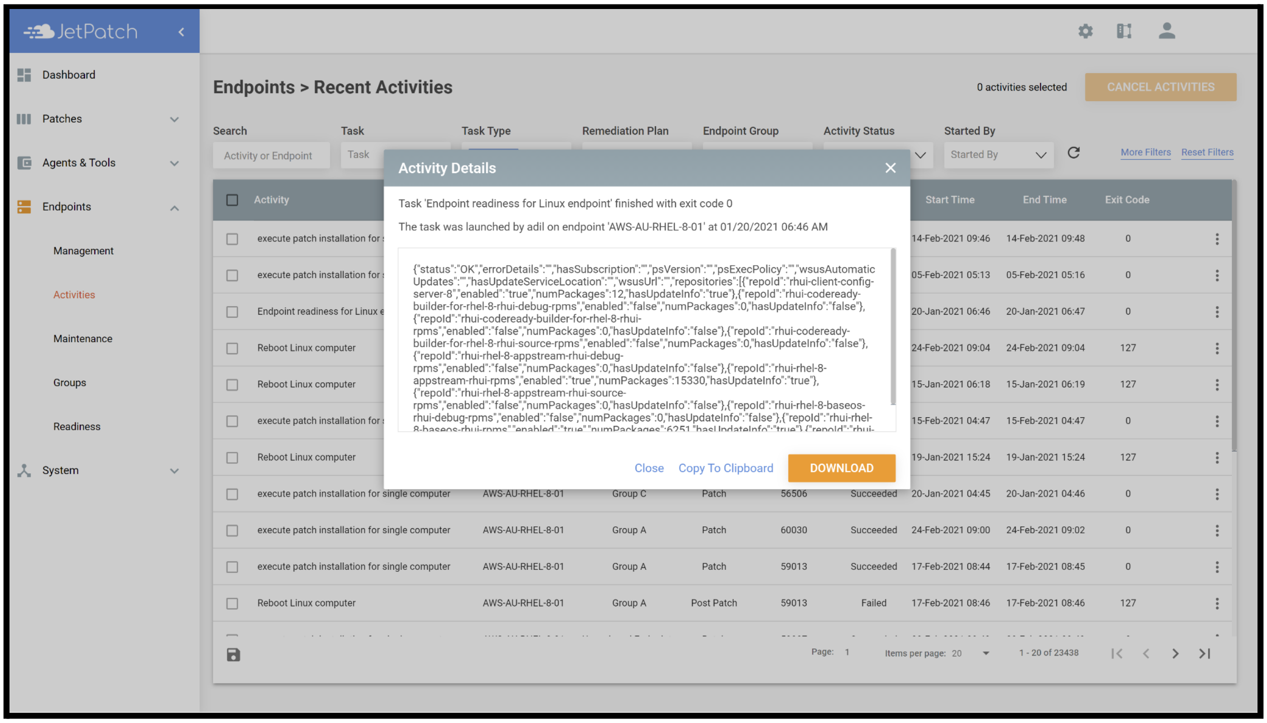
Endpoint Name	Remediation Plan	Endpoint Gr		↑	Last Reboot Time	Vulnerability Scan	Exemption	Activities
Win10-Test1	None	TestGroup			24-Feb-2021 14:34			0 | 0 | 12
Win2016-Test2	None	TestGroup			24-Feb-2021 12:37			0 | 0 | 20
TorenTimratPC	None	Unassigned Endpoints			12-Feb-2021 17:14			0 | 0 | 5
AWS-AU-RHEL-8-01	None	Group A	Red Hat Enterprise Linux 8.x	70.39%	05-Jan-2021 02:28			0 | 0 | 87
AWS-AU-RHEL-8-02	None	Group A	Red Hat Enterprise Linux 8.x	70.39%	05-Jan-2021 02:28			0 | 0 | 88
AWS-AU-RHEL-8-03	None	Unassigned Endpoints	Red Hat Enterprise Linux 8.x	71.6%	17-Feb-2021 07:55			0 | 0 | 83

Page: 1 Items per page: 20 1 - 20 of 93

Step 1: Go to *Endpoints → Management*
Step 2: Select the *Floppy Disc* icon, select *Endpoints with Missing Patches* and then *Download*
Step 3: Once downloaded, the severity column can be filtered to find critical patches

Troubleshooting

How do I check if my Patching Process has Failed?



Endpoints > Recent Activities

0 activities selected

Search: Activity or Endpoint

Task: Task

Task Type

Remediation Plan

Endpoint Group

Activity Status

Started By: Started By

Activity Details

Task 'Endpoint readiness for Linux endpoint' finished with exit code 0

The task was launched by adil on endpoint 'AWS-AU-RHEL-8-01' at 01/20/2021 06:46 AM

```
{"status":"OK","errorDetails":"","hasSubscription":"","psVersion":"","psExecPolicy":"","wsusAutomatic
Updates":"","hasUpdateServiceLocation":"","wsusUrl":"","repositories":[{"repoId":"rhui-client-config-
server-8","enabled":"true","numPackages":12,"hasUpdateInfo":"true"},{"repoId":"rhui-codeready-
builder-for-rhel-8-rhui-debug-rpms","enabled":"false","numPackages":0,"hasUpdateInfo":"false"},
{"repoId":"rhui-codeready-builder-for-rhel-8-rhui-
rpms","enabled":"false","numPackages":0,"hasUpdateInfo":"false"},{"repoId":"rhui-codeready-
builder-for-rhel-8-rhui-source-rpms","enabled":"false","numPackages":0,"hasUpdateInfo":"false"},
{"repoId":"rhui-rhel-8-appstream-rhui-debug-
rpms","enabled":"false","numPackages":0,"hasUpdateInfo":"false"},{"repoId":"rhui-rhel-8-
appstream-rhui-rpms","enabled":"true","numPackages":15330,"hasUpdateInfo":"true"},
{"repoId":"rhui-rhel-8-appstream-rhui-source-
rpms","enabled":"false","numPackages":0,"hasUpdateInfo":"false"},{"repoId":"rhui-rhel-8-baseos-
rhui-debug-rpms","enabled":"false","numPackages":0,"hasUpdateInfo":"false"},{"repoId":"rhui-rhel-
8-baseos-rhui-rpms","enabled":"true","numPackages":6251,"hasUpdateInfo":"true"},{"repoId":"rhui-
```

Activity						Start Time	End Time	Exit Code
execute patch installation for						14-Feb-2021 09:46	14-Feb-2021 09:48	0
execute patch installation for						05-Feb-2021 05:13	05-Feb-2021 05:16	0
Endpoint readiness for Linux e						20-Jan-2021 06:46	20-Jan-2021 06:47	0
Reboot Linux computer						24-Feb-2021 09:04	24-Feb-2021 09:04	127
Reboot Linux computer						15-Jan-2021 06:18	15-Jan-2021 06:19	127
execute patch installation for						15-Feb-2021 04:47	15-Feb-2021 04:47	0
Reboot Linux computer						19-Jan-2021 15:24	19-Jan-2021 15:24	127
execute patch installation for single computer	AWS-AU-RHEL-8-01	Group C	Patch	56506	Succeeded	20-Jan-2021 04:45	20-Jan-2021 04:46	0
execute patch installation for single computer	AWS-AU-RHEL-8-01	Group A	Patch	60030	Succeeded	24-Feb-2021 09:00	24-Feb-2021 09:02	0
execute patch installation for single computer	AWS-AU-RHEL-8-01	Group A	Patch	59013	Succeeded	17-Feb-2021 08:44	17-Feb-2021 08:45	0
Reboot Linux computer	AWS-AU-RHEL-8-01	Group A	Post Patch	59013	Failed	17-Feb-2021 08:46	17-Feb-2021 08:46	127

Page: 1 Items per page: 20 1 - 20 of 23438

Step 1: Go to *Endpoints* → *Activities*
Step 2: Filter on specific endpoints or remediation plan
Step 3: View the status column
Step 4: If failed, go to the right side of the row, select the 3 dots and select *View Details*. This will give more details into what might have failed