Jetpatch FAQ Guide



Table of Contents

Introduction

Inventory Setup & Policies

- How do I set a baseline for my endpoints compliance?
- Where do I see my endpoint compliance versus the baseline?
- How do I set limitations on endpoints for what they can and cannot patch?
- I added a new endpoint to a group. How do I make sure the endpoint deploys all patches already approved for the group?
- How do I exclude specific endpoints from my patching cycle?

Predictive Patching

• How do I know my patching success rate in my upcoming remediation cycle? Intelligent Workflow (Pre and Post Patching)

- How do I add specific tasks to be executed automatically before and after patching?
- How do I restart my systems automatically or at a specific time?

Automatic Remediation (Zero-Touch Remediation)

- How do I deploy patches automatically at a selected time?
 Selective Remediation
 - How do I deploy individual and/or groups of patches?
 - How do I create a remediation plan based on my vulnerability scanner report?
 - How do I rollback patches or a completed remediation plan?

Emergency Remediation

• How do I deploy an immediate patch in my environment (Zero-day Patching)? Reporting

- Reporting the compliance of my in progress or finished remediation plans?
- Reporting on patching SLAs?
- Reporting on systems missing critical patches?

Troubleshooting

• How do I check if my patching process has failed?



| æJetPatch < | | | | | | | Cu | stom Compliance is | on 🗘 | II 🚨 |
|-------------------------|--|-------------------------------------|-------------------------------|-----------|----------------|-------------------|---------------------|--------------------|---------------------------|---------------------------|
| Dashboard | Patches > Catalog | | | | 0 patches | selected | | | V | JLNERABILITY 🗸 |
| Patches ^ | | | | | | | | | | |
| Remediation Plans | Search Included Excluded Approval Status | Operating Sy | rstem Endpoint | t Name | Endpoint Group | Reme | diation Plan | Show Patches | | |
| Patches Catalog | Search Include Not A × | +3 V Operating S | ystern 🗸 Endpoin | it Name 🗸 | Endpoint Group | Rem | ediation Plan 🗸 | Not In × | \sim | More Filters Reset Filter |
| Predictive Patching NEW | Patch Title | Operating System | Product | Category | Severity CVE | Release Date ↓ | Remediation Plan | Needed On | Vulnerability Provider | y Approval Status |
| Agents & Tools 🛛 🗸 🗸 | UBUM-JP:2031 focal-updates main | Ubuntu Server 20.x x64 | Ubuntu Server Focal | Updates | Unspecified | - | | 1 | | Not Approved |
| Endpoints V | UBSM-JP:2021 focal-security main | Ubuntu Server 20.x x64 | Ubuntu Server Focal | Security | Unspecified | | | 1 | | Not Approved |
| 0 | UBUM-JP:1831 bionic-updates main | Ubuntu Server 18.x x64 | Ubuntu Server Bionic | Updates | Unspecified | - | | 1 | | Not Approved |
| System V | 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 | | 2 | | Not Approved |
| | Google Chrome 88.0.4324.190 for x64 | Windows x64 | Chrome | Updates | Unspecified | 24-Feb-2021 | | 2 | | Not Approved |
| | Zoom 5.5.2 | Windows | Zoom | Updates | Unspecified | 24-Feb-2021 | | 2 | | Not Approved |

How do I set a Baseline for my Endpoints Compliance?

Step 1: Go to Patches \rightarrow 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* \rightarrow *Servers*



| Sor | ver Acti | 000 | Manage | Tage | Filters (2) • | Manage Sm | art Groupe • | | | | | (1) | | | | | ß | Report - | JetPate | |
|-----|-----------|------|--------|---------|---------------|-----------|------------------|-----|------------|-----------|------|---------------|---------------|---------|-------------|-------------|---|----------|----------|-------------------------|
| | | Name | | | Hostna | - | | % C | Memory I | Disk Spac | Rahl | Alert jint | L Ita L Itati | a l ilo | u ğı | alcc | | × | | Mhrc |
| | 0. | Win | Type | 3.249.1 | | Window | (All Co ×) (T ×) | | 737.91 MiB | 20.17 GiB | Z | Moore Lines | i [0] [0.0 | a furre | | <u>></u> | | | M | •94 |
| | | Win | ň | 3.250.8 | | Window | All Co × T × | | 560.33 MiB | 24.19 GiB | | | i | | | | | | | |
| | * | Win | ň | 52.18.1 | | Window | All Co × T × | | 1.19 GiB | 24.95 GiB | | | i | | | <u>8.</u> | | 10 | | |
| | * | Win | i i | 34.241 | | Window | All Co ×) (T ×) | | 1.64 GiB | 15.87 GiB | | | i | | | <u>×</u> | 2 | 10 | | - L |
| | * | WIN | Û | 34.243 | | Window | (All C ×) (Wi ×) | | 615.56 MiB | 23.85 GiB | | | i | | | <u>×.</u> | 2 | 2 | | \mathbf{N} |
| | * | WIN | Û | 63.33.2 | WIN-EP-2 | Window | All C × Wi × | 7 % | 857.36 MiB | 23.62 GiB | | | i | | 49 | 5 | 2 | 10 | | $\overline{\mathbf{N}}$ |
| | * | WIN | Û | 34.241 | WIN-EP-3 | Window | (All C ×) (Wi ×) | 2 % | 821.56 MiB | 24.33 GiB | Z | | i | | | <u>×.</u> | 2 | 10 | | N |
| | * | WIN | 1 | 52.213 | WIN-EP-4 | Window | (All C ×) (Wi ×) | 4 % | 829.64 MiB | 25.18 GiB | Z | | i | | 46 | <u>×</u> | ~ | 10 | | \mathbf{N} |
| | | | | | | | | | | | | | | | | | | | | |
| Rec | ent Activ | ity | Open + | | | | | | | | | | | | | | | | | |

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 \rightarrow System \rightarrow Compliance --



| -1 | S JetPatch | < | | | | | | | \$ | E . | |
|----|-----------------------|---|------------------------|---------------------|-----------------|---|--------|------------------------|---------------|------------|---------------|
| == | Dashboard | | Compliance | | | | | | | | |
| | Patches | ~ | Add Compliance rule to | o customize your de | sired compliant | ce calculation, using endpoint tags and saved patch filters | | | _ | | _ |
| C | Agents & Tools | ~ | Search | Tags | Patch Filt | Create Compliance Rule | | | + A[| D EXCLUSIO | NRULE |
| = | Endpoints | ~ | Search | Tags | Patch Filt | Rule Name * Rule disabled | Off | | | | Reset Filters |
| x | System | ^ | Name ↑ | Description | Tag | Rule name Description | | Last Modified Affec | cted Endpoint | 5 | |
| | Compliance | | Exclude Kernel Patches | | Exclude Kernel | Rule description | | 23-Feb-2021 | 11 | | : |
| | Endpoint Groups | | | | | | | Items per page: 20 🔻 1 | 1 - 1 of 1 | < < > | >> |
| | Maintenance Schedules | | | | | Endpoints Tag * Select endpoints tag | \sim | | | | |
| | Workflows | | | | | Patch Filters * Select patch filters | \sim | | | | |
| | Tasks | | | | | Close CREATE | | | | | |
| | Scripts | | | | | | - | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |

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?

| - JetPatch | < | | | | | | | \$ | E 🚣 |
|----------------|---|-------------------------|--|--------------|--|--|--|--|---|
| Dashboard | | Endpoints Readiness | | | | Last synce | d: 24-Feb-2021 14:48 | | SETTINGS |
| Patches | ~ | Search Operatin | g System Family End | aint Crown | Unmet Criteria | Endpoint Readiness | | | |
| Agents & Tools | ~ | Server Name All X | | Ipoint Group | Unmet Criteria V | | C | | Reset Filters |
| Endpoints | ^ | | | End | oints Readiness | | | Jnmet Criteria | |
| Management | | | | | | | 2 1 2 | Conne | rctor Ready iges Ready |
| Activities | | 60 % Total readiness | | 12 | | | | 5 • Advise • Repos | ories Ready itory Ready rsion Ready |
| Maintenance | | rotai readiness | | | 18 | | 12 | 3 Subsc | ription Ready licy Ready |
| Groups | | | | Ready | Unknown | Not Ready | | | |
| Readiness | | Endpoint 1 | Connector | Subscription | Advisories Ready | Packages Support | Repository Configured | Last Reported | Endpoint Readiness |
| 🙏 System | ~ | AWS-AU-RHEL-8-01 | | - | Image: A second s | Image: A second s | Image: A second s | 24-Feb-2021 14:48 | 100% |
| | | AWS-AU-RHEL-8-02 | Image: A second s | _ | Image: A second s | Image: A second s | Image: A second s | 24-Feb-2021 14:48 | 100% |
| | | AWS-AU-RHEL-8-03 | Image: A set of the set of the | _ | Image: A second s | Image: A set of the set of the | Image: A second s | 24-Feb-2021 14:48 | 100% |
| | | AWS-UK-RHEL-7-01 | ~ | _ | Image: A second s | Image: A second s | Image: A second s | 24-Feb-2021 14:48 | 100% |
| | | | ~ | _ | Image: A second s | × | Image: A second s | 24-Feb-2021 14:48 | 100% |
| | | AWS-UK-RHEL-7-02 | | | | | | | |
| | | AWS-UK-RHEL-7-02 | · · · · · · · · · · · · · · · · · · · | - | ~ | Image: A second s | Image: A second s | 24-Feb-2021 14:48 | 100% |
| | | | | - | ✓ ✓ | ✓ ✓ | ✓ ✓ | 24-Feb-2021 14:48 24-Feb-2021 14:48 | 100% |

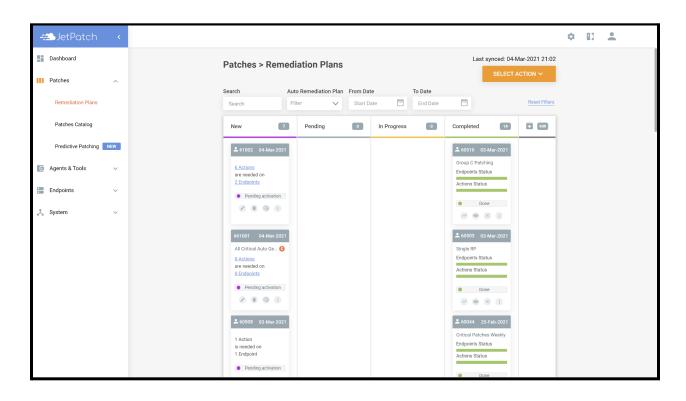
Step 1: Go to *Endpoints* \rightarrow *Readiness*

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?

| -=== JetPatch | < | | | | | | Custom Compliance is on | L 🛓 |
|--|---|--|---|--|--|--------|--|--|
| Dashboard | | Endpoints > M | anagement | | Set Suspension Definitions | | 1 endpoint selected | SELECT ACTION ~ |
| Patches Agents & Tools Endpoints Management Activities | ~ | Search Search Endpoint Name Win2016-Test2 | Remediation Plan V Remediation Plan V Remediation Plan None | Endpoint Endpoint Endpoint Gro <u>TestGroup</u> | Please choose or remove suspension for selecter endpoints | d • | tch Status Exemption atch Status Exemption Exemption Case Contemption Case Contem | More Filters Reset Filters atton Activities 010115 : |
| Maintenance Groups | | Win10-Test1 TorenTimratPC | None | TestGroup Unassigne Endpoints | Start Date * End Date * | SION | 24-Feb-2021 14:34 12-Feb-2021 17:14 | 01017 |
| Readiness | ~ | AWS-AU-RHEL-8-01 | None | <u>Group A</u> | Red Hat Enterprise Linux 8.x | 70.39% | 05-Jan-2021 02:28 | 0 0 84 |
| | | AWS-AU-RHEL-8-02 | None | <u>Group A</u> | Red Hat Enterprise Linux 8.x | 70.39% | 05-Jan-2021 02:28 | 0 0 85 |
| | | AWS-AU-RHEL-8-03 | None | <u>Unassigner</u> Endpoints | Red Hat Enterprise Linux 8.x | 71.6% | 17-Feb-2021 07:55 | 0 0 82 |
| | | 8 | | | | Pa | age: 1 Items per page: 20 ▼ 1 - 20 of 95 | < < > > |

Step 1: Go to *Endpoints* \rightarrow *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?

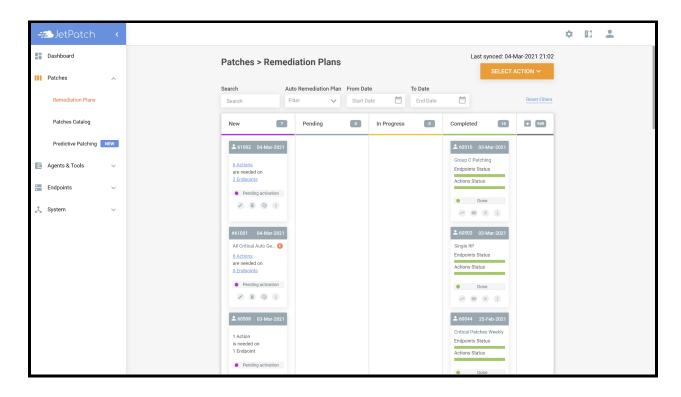
| -#=>JetPatch < | | • II ± |
|-------------------------|--|--------------------------------|
| Dashboard | Predictive Patching | |
| Patches | Let us analyze your environment or remediation plan and predict its patching success rates | |
| Remediation Plans | Environment Remediation Plan | |
| Patches Catalog | Operating System Endpoint Group | |
| Predictive Patching NEW | Operating System V Endpoint Group V Reset Filters | |
| Agents & Tools ~ | — (— — | _ |
| Endpoints ~ | | 1. |
| 🙏 System 🗸 🗸 | Calculate applicable endpoints Retrieve dependencies Analyze patches catalog Scan endpoints statuses | Predict patching success rates |
| | RUN PATCHING SIMULATION | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

Step 1: Go to Patches \rightarrow 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 $Patches \rightarrow Remediation Plans$ 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?

| -==>JetPatch | < | | | | | | : | ¢ El | • |
|---------------------|----|---------------------|-------------------------------------|------------------|-------------------|----------------------------|-------------------|----------|-------------------|
| Dashboard | | System > Workflows | | | | | | + CREATE | WORKFLOW |
| Patches | ~ | Search | | | | | | | |
| Agents & Tools | ~ | Search | | | | | | | Reset Filters |
| Endpoints | ~ | Workflow Name | Description ↑ | Operating System | Created On | Status | Created By | | |
| Management | | Application Testing | | Windows | 22-Dec-2020 10:23 | • Idle | smolnik | | : |
| Activities | | Lab Workflow | | Linux | 10-Aug-2020 04:41 | Active | smolnik | | : |
| Activities | | Reboot Linux | - | Linux(Default) | 24-0ct-2019 11:54 | Active | tkirkland | | : |
| Maintenance | | Reboot Windows | | Windows(Default) | 24-0ct-2019 11:54 | Active | tkirkland | | : |
| Groups | | Restart Machine | - | Windows | 04-Aug-2020 13:28 | Active | tom (deleted) | | : |
| Readiness | | test | - | Windows | 17-Feb-2021 08:37 | Idle | ndoganis | | : |
| 🙏 System | ~ | test 16 feb | - | Linux | 16-Feb-2021 04:52 | • Idle | ndoganis | | : |
| | | test WF 24 February | | Windows | 24-Feb-2021 08:59 | Idle | ndoganis | | : |
| Compliance | | Webinar 09 Dec | - | Windows | 23-Nov-2020 03:50 | • Idle | ndoganis | | : |
| Endpoint Groups | | Patch Solaris | Automatically created by the system | Solaris(Default) | 19-Feb-2020 17:37 | Active | Policy Manager | | : |
| Maintenance Schedul | es | | | | Page: 1 | Items per page | 20 🔻 1 - 10 of 10 | < - | (\rightarrow) |
| Workflows | | | | | | | | | |
| Tasks | , | | | | | | | | |

Step 1: Go to Systems \rightarrow 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?

| Endpoints > Manager Run Task On Endpoint × | 1 endpoint selected | SELECT ACTION ~ |
|---|--|----------------------------|
| Patches V Search Remedia Please select a task to run on selected endpoints | Exemption | |
| Agents & Tools Search Remedi Filter By Select Task | Exemption V | More Filters Reset Filters |
| Endpoints Endpoint Name P Category reboot Filter by Category Advanced Windows Reboot | boot Vulnerability Exemption e Scan | on Activities |
| Management Win10-Test1 Created By Created By Check if Windows Reboot is Required and Filter by Creator V Interactive reboot Duilt in service | 21 14:34 | 0 0 12 |
| Activities Linux_reboot_init6 Linux_reboot_init6 Phease note that tacks based soriets with specified operating system will run only on eligible endpoints Simple Windows Reboot | 21 12:37 | 0 0 20 |
| Groups TorenTimratPC N | 21 17:14 | 01015 |
| Readiness Timezone * Date & Time * AWS-AU-RHEL-8-01 N Select timezone Select date & time | 21 02:28 | 0 0 87 |
| Close RUN TASK | 21 02:28 | 0 0 88 |
| AWS-AU-RHEL-8-03 None Unassigned Red Hat Enterprise Linux 71.6% 17-Feb-2 | 2021 07:55 | 0 0 83 |
| Page: 1 Herr | ns per page: 20 💌 1 - 20 of 93 | I< < > >I |

Step 1: Go to *Endpoints* \rightarrow *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

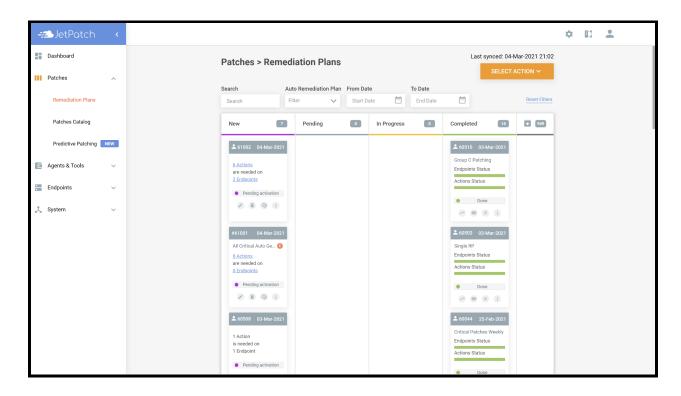
How do I deploy Patches Automatically at a Select Time?

| Æ JetPatch | < | | | | | Custom Complia | nce is on | • |
|---------------------|-----|---|--|----------------------------------|--------------------|--------------------------------------|------------------------|-------------------|
| Dashboard | | Patches > Catalog | | | 0 patches selected | + CREATE REMEDIATION | PLAN VULNERAE | BILITY ~ |
| Patches | ^ | | | | | | | |
| Remediation Plans | | Search Included Excluded Approval Statu | s Operating System E | Indpoint Name | Endpoint Group | Remediation Plan Show Pate | hes | |
| Patches Catalog | | Search Include Install × | ✓ Operating System ✓ | Endpoint Name 🗸 🗸 | Endpoint Group 🗸 🗸 | Remediation Plan 🗸 Show Pat | ches 🗸 More Filte | ers Reset Filters |
| Predictive Patching | NEW | Patch Title | | | Severity CVE Reli | ease R∉ More Filters ate ↓ | | pproval Status |
| Agents & Tools | ~ | RHBA-2020:2662 selinux-policy bug fix and enhancement update | Red Hat Enterprise Linux : Linux 7.x x64 7, Red Hat En Linux : | terprise Bug Fix | Unspecified 23-Ju | IN-2020 To Date | Start Date | Install |
| Endpoints | ~ | RHBA-2020:2660 rsyslog bug fix and enhancement update | Red Hat Enter Red Hat Enterprise Linux 3 Linux 7.x x64 7, Red Hat En | erprise 7 Bug Fix terprise | Unspecified 23-Ju | n-2020 Released Before | Days | Install |
| 🏃 System | ~ | RHBA-2020:2659 systemd bug fix and enhancement update | Linux : Red Hat Ent Red Hat Enterprise Linux : Linux 7.x x64 7, Red Hat En Linux : | erprise 7 Bug Fix terprise | Unspecified 23-Ju | Released In The La | st Days Severity V | Install |
| | | RHBA-2020:2654 cloud-init bug fix and enhancement update | Red Hat Ent Red Hat Enterprise Linux : Linux 7.x x64 7, Red Hat En Linux : | 7 Bug Fix terprise | Unspecified 23-Ju | Category In-2020 Vulnerability | Category Vulnerability | Install |
| | | RHSA-2020:2432 Moderate: microcode_ctl security, bug fix and enhancement update | Red Hat Enter Red Hat Enterprise Linux : Linux 7.x x64 7, Red Hat En Linux : | 7 Security terprise | Moderate 09-Ju | Product in-2020 | Product V | Install |
| | | 2020-06 Servicing Stack Update for Windows Server 2012 R2 for x64-based Systems (KB4562253) | Windows Server 2012 Windows Serv R2 x64 R2 | ver 2012 Security Updates | Critical 09-Ju | in-2020 0 | _ | Install |
| | | 2020-06 Security Only Quality Update for Windows Server 2012 R2 for x64-based Systems (KB4561673) | Windows Server 2012 Windows Serv R2 x64 R2 | ver 2012 Security Updates | Critical 09-Ju | in-2020 0 | | Install |
| | | 2020-06 Cumulative Security Update for | ue. J 0 | | Page: | 1 Items per page: 20 💌 | 1 - 20 of 627 < < | > >1 |

Step 1: Go to Patches \rightarrow 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* \rightarrow *Remediation Plans*





Step 5: Select Action \rightarrow Create/Edit Remediation Plan Rules



| -:: | JetPatch | < | | | | | | ۵ | II 🔺 |
|-----|-----------------------------------|-----|---|--|----------|---|-----------------------------------|-----------------------|---------------|
| D. | ashboard | | Automatic Rer | nediation Plans | Rules | Create Automatic Remediation Plan Rule | < | | |
| P. | atches Remediation Plans | ^ | | ediation Plans rules base mediation Plans for ena | | Rule Name * Automatic Creation | | | |
| | Patches Catalog | | + ADD RULE Search | Patch Filter | Modified | Patch Filter * Select Patch Filter | ion From Date | Next Creation To Date | |
| | Predictive Patching gents & Tools | NEW | Search Name ↑ | Patch Filter V | Modified | Repeat every * | te 💼 | End Date | Reset Filters |
| _ | ndpoints | ~ | All Critical | All Critical | Todd | Timezone * Select timezone |)0:00 vay | No | : |
| 🙏 s | ystem | ~ | Critical and 60 days Critical and more than 10 | Critical >60 day days Critical >10 day | | Create a plan now Activate the plan on creation | 00:00 vay 00:00 | No | : |
| | | | nexpose auto plan | Nexpose Filter | Todd | Workflow * Please note the Workflows will apply on all Endpoint Groups Windows Reboot Windows |)0:00 vay Items per page: 2 | No 20 ▼ 1-4 of 4 | : |
| | | | | | _ | Close SAVE | nema per page. 2 | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |

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?

| +=>JetPatch | < | | | | | Cu | stom Compliance is on | ¢ 🗉 💄 |
|---------------------|-----|---|---|----------------------------|---------------------|---------------------|-----------------------|--|
| Dashboard | | Patches > Catalog | | | 0 patches selected | + CREATE REN | | VULNERABILITY ~ |
| Patches | ^ | | | | | | | |
| Remediation Plans | | Search Included Excluded Approval Statu | s Operating System | Endpoint Name | Endpoint Group F | Remediation Plan | Show Patches | |
| Patches Catalog | | Search Include Install × | ✓ Operating System ✓ | Endpoint Name 🗸 🗸 | Endpoint Group 🗸 🗸 | Remediation Plan 🗸 | Show Patches | More Filters Reset Filters |
| Predictive Patching | NEW | Patch Title | Operating System Prod | uct Category | Severity CVE Relea | | Needed V On | ulnerability Approval Provider Status |
| Agents & Tools | ~ | RHBA-2020:2662 selinux-policy bug fix and enhancement update | Red Hat Enterprise Linux Linux 7.x x64 7, Red Hat E Linux | Enterprise Bug Fix | Unspecified 23-Jun- | 2020 55509 | 0 | Install |
| Endpoints | × | RHBA-2020:2660 rsyslog bug fix and enhancement update | Red Hat Erterprise Linux Linux 7.x x64 7, Red Hat E Linux 7.x x64 7, Red Hat E Linux | x 7 Bug Fix Enterprise | Unspecified 23-Jun- | 2020 55509 | 1 | Install |
| - Gouin | Ť | RHBA-2020:2659 systemd bug fix and enhancement update | Red Hat Enterprise Linux Linux 7.x x64 7, Red Hat E Linux 7.x x64 7, Red Hat E | x 7 Bug Fix Enterprise | Unspecified 23-Jun- | 2020 55509 | 1 | Install |
| | | RHBA-2020:2654 cloud-init bug fix and enhancement update | Red Hat Enterprise Linux Linux 7.x x64 7, Red Hat E Linux 7.x inux 7.x k64 7, Red Hat E | x 7 Bug Fix Enterprise | Unspecified 23-Jun- | 2020 | 0 | Install |
| | | RHSA-2020:2432 Moderate: microcode_ctl security, bug fix and enhancement update | Red Hat Erterprise Linux Linux 7.x x64 7, Red Hat E Linux 7.x inux 7.x Linux | x 7 Security Enterprise | Moderate 09-Jun- | 2020 | 0 | Install |
| | | 2020-06 Servicing Stack Update for Windows Server 2012 R2 for x64-based Systems (KB4562253) | Windows Server 2012 Windows Se R2 x64 R2 | | 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 Windows Se R2 x64 R2 | | Critical 09-Jun- | 2020 | 0 | Install |
| | | 2020-06 Cumulative Security Update for | ut.JAAMA Ut.JA. | | Page: | I Items per page: 2 | 20 💌 1 - 20 of 6: | 27 < < > > |

Step 1: Go to Patches \rightarrow 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 Filters* 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?

| -£ JetPatch | < | | | | | | | Custo | om Compliance is on | • 🛙 🕹 | • |
|-----------------------|---|-------------------------|-------------------------------|-------------------|------------------------|--------------------|--------------------------|--|---|----------------------|-------------|
| Dashboard | | Endpoints > Ma | nagement | | | | | | 0 endpoints se | lected SELECT | |
| Patches | ~ | Search | Remediation Plan | Endpoint Group | Operating Syste | m Patch | Patch St | atus Exem | ption | | |
| Agents & Tools | ~ | Search | Remediation Plan \checkmark | Endpoint Group | Operating Syste | m 🗸 🦳 Patch | V Patch S | tatus 🗸 Exen | nption 🗸 | More Filters | Reset Filte |
| Endpoints | ^ | Endpoint Name | Remediation Plan | | | Patching Status | Endpoint 1 Compliance | Last Reboot Time | Vulnerability Scan | | |
| Management | | WIN-EP-3 | None | US Windows | Windows Server 2012 R2 | | 78.57% | 18-Feb-2021 02:54 | Nessus: <u>3</u> / <u>3</u> Nexpose: <u>0</u> / <u>0</u> | 0 0 31 | * * |
| Activities | | WIN-EP-1 | None | UK Windows | Windows Server 2012 R2 | | 79.87% | 22-Feb-2021 01:18 | Nexpose: 0 / 0 | 0 0 159 | : |
| Maintenance Groups | | WIN-EP-2 | None | <u>UK Windows</u> | Windows Server 2012 R2 | | 79.87% | 22-Feb-2021 01:20 | Nexpose: 0 / 0 | 0 0 149 | : |
| Readiness | | AWS-US-CentOS-7-1 | None | Group B | CentOS 7.x | - | 81.25% | 24-Feb-2021 12:40 | | 0 0 94 | ** |
| System | ~ | 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 | <u>Group B</u> | 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% Page: 1 | 29 Jan-2021 00:27 Items per page: 2 | 0 💌 1-20 | 010182 of 94 < < | > > |

Step 1: Go to *Endpoints* \rightarrow *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

| | | Custom Compliance is on |
|-------------------------|--|---|
| Dashboard | Patches > Catalog | 0 patches selected + CREATE REMEDIATION PLAN VULNERABILITY ~ |
| Patches ^ | च saved filters ∽ | |
| Remediation Plans | Search Included Excluded Approval Status Operating System Endpoint Name | Endpoint Group Remediation Plan Show Patches |
| Patches Catalog | Search Include Operating System V Endpoint Name V | Endpoint Group V Remediation Plan V Show Patches V More Filters Reset Filter |
| Predictive Patching NEW | Patch Title Operating System Product Category | Severity CVE Release J Remediation Needed Vulnerability Approval Date J Plan On Provider Status |
| Agents & Tools ~ | RHBA-2020-2662 selinux-policy bug fix and enhancement update Red Hat Enterprise Linux 7.x x64 Linux 7 Bug Fix | Unspecified 23-Jun-2020 55509 0 Install |
| Endpoints V | Red Hat Enterprise RHBA-2020:2660 rsyslog bug fix and Red Hat Enterprise Linux 7 x x64 Red Hat Enterprise Red Hat Enterpris | Unspecified 23-Jun-2020 55509 1 Install |
| 🙏 System 🗸 🗸 | Red Hat Enterprise HBA-2020.2659 systemd bug fix and Red Hat Enterprise Linux 7 x x64 Hat Enterprise Linux 7 x x64 Hat Enterprise Linux 7 | Unspecified 23-Jun-2020 55509 <u>1</u> Install |
| | Red Hat Enterprise RHBA-2020.2654 cloud-init bug fix and enhancement update Red Hat Enterprise Linux 7 Red Hat Enterprise Linux 7 Red Hat Enterprise | Unspecified 23 Jun 2020 0 Install |
| | Red Hat Enterprise Linux 7 Red Hat Enterprise Linux 7 | Moderate 09-Jun-2020 0 Install |
| | 2020-06 Servicing Stack Update for Windows Windows Server 2012 Security Server 2012 R2 for x64-based Systems R2 x64 R2 Updates | Critical 09-Jun-2020 0 install |
| | 2020-06 Security Only Quality Update for Windows Server 2012 R2 for x64-based Systems (R4556163) | Critical 09-Jun-2020 0 Install |
| | 2020-06 Cumulative Security Update for | Page: 1 ttems per page: 20 ▼ 1-20 of 627 < < >> |

Step 1: Go to Patches \rightarrow 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

| | | • 🗉 🔺 |
|-------------------------|--|-------|
| Dashboard | Patches > Remediation Plans | |
| Patches | Search Auto Remediation Plan From Date To Date | |
| Remediation Plans | Search Filter V Start Date End Date End Date | |
| Patches Catalog | New S Pending O In Progress O Completed 11 S P45 | |
| Predictive Patching NEW | ± 60043 25-Feb-2021 | |
| Agents & Tools 🗸 | Test Group Patching 1 Action Endpoints Status is needed on | |
| Endpoints 🗸 | Actions Status Actions Status Done | |
| 🙏 System 🗸 | | |
| | #60047 26-Feb-2021 #60041 25-Feb | |
| | All Critical Auto Ge O B I M Auto General Archive 3 Actions Endpoints Status | |
| | are needed on Actions Status | |
| | Pending activation Done | |
| | | |
| | #60045 25-Feb-2021 | |
| | Rapid weekly Auto Ge zoom 7 Actions Endpoints Status | |
| | Actions are needed on <u>4 Endpoints Actions Status </u> | |
| | Pending activation Done | |

Step 1: Go to Patches \rightarrow 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)?

| -#_>JetPatch | < | | | | Custom Compliance is | on 🌣 🛄 💄 |
|---------------------|-----|---|--|-------------------------------|---------------------------------|---|
| Dashboard | | Patches > Catalog | | 0 patches selected | + CREATE REMEDIATION PLAN | N VULNERABILITY ~ |
| Patches | ^ | | | | | |
| Remediation Plans | | Search Included Excluded Approval Statu | s Operating System Endpoint Name | Endpoint Group Re | emediation Plan Show Patches | |
| Patches Catalog | | Search Include Install × | ✓ Operating System ✓ Endpoint Name ✓ | Endpoint Group V | Remediation Plan 🗸 Show Patches | More Filters Reset Filters |
| Predictive Patching | NEW | Patch Title | Operating System Product Categor | y Severity CVE Releas Date | | Vulnerability Approval Provider Status |
| Agents & Tools | ~ | RHBA-2020:2662 selinux-policy bug fix and enhancement update | Red Hat Enterprise Linux 7 Linux 7.x x64 7, Red Hat Enterprise Bug Fix Linux 7 | Unspecified 23-Jun-2 | 020 55509 0 | Install |
| Endpoints | ~ | RHBA-2020:2660 rsyslog bug fix and enhancement update | Red Hat Enterprise Red Hat Enterprise Linux 7 Linux 7,x x64 7, Red Hat Enterprise Linux 7 | Unspecified 23-Jun-2 | 020 55509 1 | Install |
| A System | Ť | RHBA-2020:2659 systemd bug fix and enhancement update | Red Hat Enterprise Red Hat Enterprise Linux 7 Bug Fib Linux 7.x x64 7, Red Hat Enterprise Linux 7 | Unspecified 23-Jun-2 | 020 55509 1 | Install |
| | | RHBA-2020:2654 cloud-init bug fix and enhancement update | Red Hat Enterprise Red Hat Enterprise Linux 7 Bug Fiv Linux 7.x x64 7, Red Hat Enterprise Linux 7 | Unspecified 23-Jun-2 | 020 0 | Install |
| | | RHSA-2020:2432 Moderate: microcode_ctl security, bug fix and enhancement update | Red Hat Enterprise Red Hat Enterprise Linux 7 Linux 7.x x64 7, Red Hat Enterprise Linux 7 | Moderate 09-Jun-2 | 020 0 | Install |
| | | 2020-06 Servicing Stack Update for Windows Server 2012 R2 for x64-based Systems (KB4562253) | Windows Server 2012 Windows Server 2012 Securit R2 x64 R2 Update | | 020 0 | Install |
| | | 2020-06 Security Only Quality Update for Windows Server 2012 R2 for x64-based Systems (KB4561673) | Windows Server 2012 Windows Server 2012 Securit R2 x64 R2 Update: | | 020 0 | install |
| | | 2020-06 Cumulative Security Update for | ue | Page: 1 | Items per page: 20 💌 1 - 2 | 0 of 627 < < > > |

Step 1: Go to System \rightarrow 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.

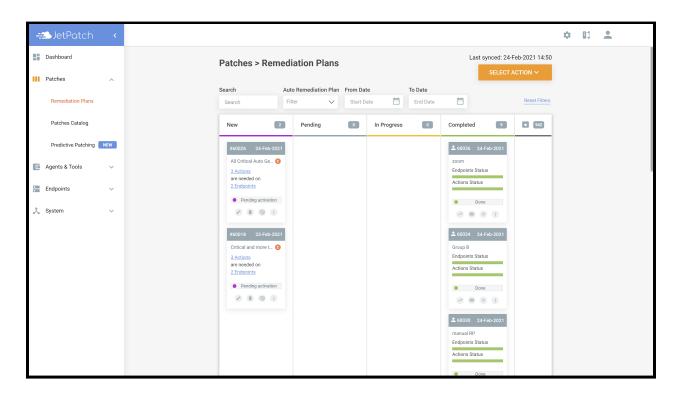
Step 7: Select the Emergency Maintenance Window

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 \rightarrow 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



| -#_>JetPatch | < | | | | | | | Custo | m Compliance is on | ¢ 🗉 🚣 | |
|-----------------------|---|-----------------------|---------------------|-------------------|------------------------|--------------------|--------------------------|--|---|--------------|-------------|
| Dashboard | | Endpoints > Ma | anagement | | | | | | 0 endpoints selec | ted SELECT | |
| Patches | ~ | Search | Remediation Plan | Endpoint Group | Operating Syster | n Patch | Patch Sta | tus Exem | ption | | |
| Agents & Tools | ~ | Search | Remediation Plan 🗸 | Endpoint Group | ✓ Operating System | n 🗸 Patch | V Patch St | atus 🗸 Exen | nption 🗸 | More Filters | Reset Filte |
| Endpoints | ~ | Endpoint Name | Remediation Plan | | | Patching Status | Endpoint f Compliance | Last Reboot Time | Vulnerability Ex Scan | | |
| Management | | AWS-US-CentOS-8- 1 | None | <u>Group C</u> | CentOS 8.x | | 75.25% | 03-Mar-2021 13:05 | | 0 0 85 | : |
| Activities | | AWS-US-CentOS-8- 2 | None | Group C | CentOS 8.x | | 75.25% | 03-Mar-2021 13:05 | | 0 0 85 | : |
| Maintenance Groups | | WIN-EP-3 | None | <u>US Windows</u> | Windows Server 2012 R2 | | 76.58% | 18-Feb-2021 02:54 | Nessus: <u>3</u> / <u>3</u> Nexpose: <u>0</u> / <u>0</u> | | : |
| Readiness | | WIN-EP-4 | None | US Windows | Windows Server 2012 R2 | | 76.58% | 28-Feb-2021 19:03 | Nessus: <u>3</u> / <u>3</u> | - | : |
| 🦕 System | ~ | 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-ED-1 | None | HK Windowe | Windowe Carvar 2012 D2 | | 70.87%. Page: 1 | 22-Fab-2021 01-18 Items per page: 2 | Nevnose: 0 / 0 ▼ 1 - 20 of 9 | - 5 < < | > >1 |

Step 4: Go to $Endpoints \rightarrow Management$

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?

| | | | ¢ 🗈 单 | | | |
|-------------------|---------------------------------------|---|---|--|--|--|
| Dashboard | Dashboards | | | | | |
| Patches 🗸 | | | | | | |
| Agents & Tools | Patches Compliance Agents Compliance | | | | | |
| Le Agents à roois | | Download SLA Summary Report × | | | | |
| Endpoints 🗸 | Patches Compliance Dashboard | The SLA report provides an overall update of all remediation plans where the SLA start/end date falls within the selected timeframe. | DOWNLOAD REPORTS 🗸 | | | |
| 🙏 System 🗸 | Operating System Endpoint Group | More information can be found in <u>Generate SLA Report</u> | | | | |
| N System V | Operating System 🗸 Endpoint Group 🗸 C | Please choose the SLA report details: | Reset Filters | | | |
| | All Operating Systems Summary | SLA: Start Date 👻 | Last synced: 04-Mar-2021 21:31 | | | |
| | 60% | Between: 3/1/2021 to 3/31/2021 | 970 Remediation plans ③ | | | |
| | Effective compliance | Close Domitoria | | | | |
| | Applicable endpoints | 28 Applicable endpoints 30 | 7 | | | |
| | Compliant endpoints | 16 Compliant endpoints 16 | | | | |
| | In progress endpoints | 0 In progress endpoints 0 | | | | |
| | Pending endpoints | 0 Pending endpoints 0 | | | | |
| | Failed endpoints | 12 Failed endpoints 12 | 963 | | | |
| | | Exempted endpoints 2 | New Pending In Progress Completed | | | |
| | Detailed Data By Operating System | | | | | |
| | 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?

| | < | | | | | | | Custom Compliance is | on 🌣 🛄 | • |
|---------------------------|---|------------------|---------------------|---------------------------------------|---|----------------|--------------|---------------------------------|---------------|-------------------------|
| Dashboard | | Endpoints > Ma | nagement | | | | | 0 endpoints | s selected SI | |
| Patches | ~ | Search | Remediation Plan | Endpoint G | roup Operating System | Patch | Patch Status | Exemption | | |
| Agents & Tools | ~ | Search | Remediation Plan 🗸 | Endpoint | Download Reports | | atch Status | Exemption | More | e Filters Reset Filters |
| Endpoints | ^ | Endpoint Name | Remediation Plan | Endpoint Gro | Please select a report to down | nload | | Reboot Vulnerability me Scan | Exemption Act | ivities |
| Management | | Win10-Test1 | None | <u>TestGroup</u> | Type CSV | | 24-Feb-2 | 021 14:34 | 0 | 0 12 |
| Activities Maintenance | | Win2016-Test2 | None | TestGroup | Report Endpoints Management Repo Endpoints with Missing Patch | es | 24-Feb-2 | 021 12:37 | 0 | 0 20 |
| Groups | | TorenTimratPC | None | Unassigne Endpoints | Endpoints with Missing Secur | Close DOWNLOAD | 12-Feb-2 | 021 17:14 | 0 | 10 5 |
| Readiness System | ~ | AWS-AU-RHEL-8-01 | None | Group A | Red Hat Enterprise Linux 8.x | 70.39 | % 05-Jan-2 | 021 02:28 | 0 | 0 87 |
| | | AWS-AU-RHEL-8-02 | None | <u>Group A</u> | Red Hat Enterprise Linux 8.x | 70.39 | % 05-Jan-2 | 021 02:28 | 0 | 0 88 |
| | | AWS-AU-RHEL-8-03 | None | <u>Unassigned</u> <u>Endpoints</u> | Red Hat Enterprise Linux 8.x | 71.69 | 6 17-Feb-2 | 021 07:55 | 0 | 0 83 |
| | | 8 | | | | | Page: 1 Iten | ns per page: 20 💌 1 - | 20 of 93 < | < > >I |

Step 1: Go to *Endpoints* \rightarrow *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?

| -# JetPatch | < | | | | | | | | | \$ | : II 4 | 2 |
|----------------|---|--------------------------------|----------------------------------|---|--|-----------------------|------------------|----------------|-------------------|-------------------|-------------|------------------------|
| Dashboard | | Endpoints > Recent | Activities | | | | | | 0 ac | tivities selected | | |
| Patches | ~ | Search Task | Ta | ask Type | Remediation Plan | Endpoint Grou | ip Ac | tivity Status: | Started By | | | |
| Agents & Tools | ~ | Activity or Endpoint Task | Activity De | tails | | | | | Started By | ~ C | More Filter | s <u>Reset Filters</u> |
| 📒 Endpoints | ~ | Activity | Task 'Endpoint | readiness for Linux | endpoint' finished witl | exit code 0 | | | Start Time | | | |
| Management | | execute patch installation for | | aunched by adil on e | ndpoint 'AWS-AU-RHE | L-8-01' at 01/20/202 | 1 06:46 AM | | 14-Feb-2021 09:46 | 14-Feb-2021 09:48 | 0 | : |
| Ŷ | | execute patch installation for | Updates":""," | hasUpdateServiceLo | sSubscription":"","psV ocation":"","wsusUrl":"", | repositories":[{"repo | ld":"rhui-client | t-config- | 05-Feb-2021 05:13 | 05-Feb-2021 05:16 | 0 | : |
| Activities | | Endpoint readiness for Linux | e builder-for-r {"repold":"rh | nabled":"true","numPa hel-8-rhui-debug-rpm uu-codeready-builder | 20-Jan-2021 06:46 | 20-Jan-2021 06:47 | 0 | : | | | | |
| Maintenance | | Reboot Linux computer | builder-for-r {"repold":"rh | led":"false","numPac hel-8-rhui-source-rpr uu-rhel-8-appstream- | 24-Feb-2021 09:04 | 24-Feb-2021 09:04 | 127 | : | | | | |
| Groups | | Reboot Linux computer | appstream- {"repold":"rh | rhui-rpms","enabled": ui-rhel-8-appstream- | | 15330,"hasUpdateIn | fo":"true"}, | | 15-Jan-2021 06:18 | 15-Jan-2021 06:19 | 127 | : |
| Readiness | | execute patch installation for | rhui-debug-r | rpms","enabled":"fals | kages":0,"hasUpdateIr e","numPackages":0,"h rue"."numPackages":6 | asUpdateInfo":"false | "}.{"repold":"rl | hui-rhel- | 15-Feb-2021 04:47 | 15-Feb-2021 04:47 | 0 | : |
| 🉏 System | ~ | Reboot Linux computer | | | Close | Copy To Clipboard | DOW | NLOAD | 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 | : |
| | | 8 | | | ··· · · <u>·</u> ···· | | Page: | 1 Item | s per page: 20 👻 | 1 - 20 of 23438 | K K | > >I |
| | | | | | | | | | | | | |

Step 1: Go to *Endpoints* \rightarrow *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

