CONESTOGA
Connect Life and Learning

Student Name:	Aagam Sanjay Shah
Deliverable:	Assignment 2
Course Name:	NTWK8180-24S-Sec3-IT Environmental Planning

Date Assigned:	29/09/2024
Date Due:	13/10/2024
Rules:	• Individual. • Cheating is not allowed. • Plagiarism counts as cheating! • That FAILURE to submit work in the course can result in a grade of ‘F’ or ‘I’ for failure to complete the course!

Table of Contents

Introduction

In any Organization updating devices and maintaining the software or applications with its patches whether it is software or hardware updates. After upgrading 300 servers to windows servers 2022 other systems and devices need to update the patches throughout the company on different devices and with various models including different versions. Maintaining IT infrastructure of a organization is crucial part. Devices, systems, machines need to be updates at regular intervals with various patches to avoid any kind of disaster, security breaches, break though in an organization. As supervisor assigned this task IT admins to come up with a deployment of patches on various levels such as networking devices, windows servers, Linux server updates. Also figuring out the downtime required to perform the updates as well as need to check if devices need to be newly purchased and so on depending on different devices for different purposes. Performing system updates though various patches and testing is necessary to ensure reliability, stability in daily operations and minimizing the risk of failure and other threats to the organization. A semi-automated patch delivery system or server needs to be deployed to handle this task. There are various software's / applications to handle this task, which applies patches/updates on wide range of hardware, user's systems. To perform this task a proper planning, downtime, documentation needs to be created before making any changes as well as recovery methods needs to be planned if any failures faced in any case.

In-Class Research

Week 1: Calculate devices and applications to deploy patches

1. Prepare Number to devices and applications

To deploy patches first we need to calculate which all devices need upgrade of hardware or software upgrades. After upgrading 300 servers some or the other patches are required to deploy for smooth operations and smooth working with applications/software's running on it. The main task is to identify how many systems, servers and other devices require patches which includes user's workstations, hardware devices and applications.

<u>Types and number of devices</u>

Windows Servers	213
Linux Servers	87
Network Devices	60
Security	12
Printer	8
Others	40
Windows System	417
Apple System	53
Linux System	35
Wi-fi devices	28

2. Patch can be categorized

Either patches can be categorized in phase wise, department wise or as critical patch updates and noncritical patch updates. After every patch there testing should be performed to assure the reliability and stability of the patch deployed.

For example, Company sends updates as Minor update, Major Update, Critical Updates. Few updates require downtime, whereas other updates require downtime with wide range of coordination with cross domain teams.

3. Backup before deploying patches

Data is the most important before making any changes or updating any devices or systems in an organization whether it is critical or noncritical. Separate backup taking confirmation needs to be taken and assures its reliable to recover in case of rollback. Every backup and update need to be monitored. Not all systems have to be backed up, but Critical devices which deals with servers, security, networking and so on to be backed up.

4. Patch testing

Before deploying any updates on any device or systems, each update has to be tested and assured the stability of it.

For Example, deploying on firewall devices, network devices or critical infrastructure, patches can be testing in UAT environments before deploying on Production environments to reduce the risk of failure.

Week 2: Patch Deployment Plan

1. OS Patches

➔ Windows Server and Windows workstations

With the help of SCCM tool used for deploying patches. This tool is used to manage download updates and deploy on the workstations and servers.

➔ Linux Servers and Linux Workstations

Deploying Patches on Linux servers and workstations third-party applications or software's are also used to perform the same.

➔ Mac OS

Each update are supposed to be documented and reviewed the performance with its cause and effects of applications before deployments.

Patches can be deployed Weekly, Bi-Weekly, Monthly or urgent/Critical update.

OS Types	**No. of Devices**	**Approx time of updating systems**
Windows Servers	213	15 days
Windows Systems	417	15 days

Linux Servers	87	1 week
Linux System	35	1 week
Apple system	53	1 week
Total	**805**	

2. Application/Firmware Patches

Devices impacted with Application or firmware patches

➔ Firewall OS update/ Patches.
➔ Database platform patches
➔ Networking devices (Router Switches)
➔ Printer
➔ Wi-fi devices (AP’s, controllers)
➔ Load balancer, storage devices etc.

Few Examples are as followed:

Microsoft patches → MS exchange, Microsoft office, windows defender updates.

Linux patches → different services and patches are downloaded and updates such as Apache, NGINX, docker and other features.

Firewall updates → Checkpoint, FortiGate, etc.

Wi-Fi devices → Aruba, Ruckus.

Networking devices → Cisco Routers, Switches, Digital Phones, etc. HP devices, Juniper, Tejas devices.

Load balancer → F5, etc.

Week 3: Recovery plan

- Workstation Patches

If any user faced any data loss or end users are not working on, if critical system the rollback is performed, and data is restored till the issue is solved.

Deployment of patches are performed in off-hours so if any impact faced, recover can be done immediately. This won’t hamper any users work or sessions. While performing this task active participation is required from support team to check and confirm the system stability whether its Linux, Windows, MAC based.

- Hardware Patch/Upgrades

Test patches on UAT environments to confirm its stability and reduce the failures. This activity is performed in nonworking hours to reduce impacts, and these devices are monitored for 24-48 hours minimum before moving to deployment on production environment.

Hardware, firmware patches need full downtime or traffic/data is shifted to secondary devices or supporting devices.

➔ Router, Switch, Firewall, Load Balancer, Wi-Fi, Database and so on.

In Case if any failure occurs, rollback is performed withing new or in the taken downtime. Further to it backup taken is restored on the same.

Plan timeline

Specifying priority to perform deployment of patches on different devices based on the criticality of the devices and department.

Below table mentioned show the priority of deploying patches and updates:

OS Types	No. of Devices	Approx time of updating systems	Priority
Windows Servers	213	15 days	1
Linux Servers	87	1 month	2
Network Devices	60	3 months	3
Security	12	1 month	4
Printer	8	1 week	9
Others	40	1 month	10
Windows System	417	15 days	6
Apple System	53	1 week	8
Linux System	35	1 week	7
Wi-Fi devices	28	15 days	5
Total	**953**	**8 months 1 week**	

The overall deployment of patches will take approximately 8 months to complete based on the priority.

Breakdown of Tasks

There are various teams, or we can say as breakdown of tasks which has to be performed throughout the activity of patch deployment.

1. Transition Team/Inventory Management Team

➔ This team keeps count of number of Servers, devices, systems, applications/software's with its license and workstation are in an organisation on which patch needs to be applies.

2. Backup Team

➔ This team will take backup of devices at regular interval based on critical and noncritical devices status.

➔ This team is responsible for managing the backups of the devices, so in-case if any failure occurs, they can immediately help with data restoration process.

3. Testing Team

➔ This team performs initial patch deployment on UAT environments to make sure about the patch deployment in Production environments.

➔ After performing test case of patch deployment on UAT environments, it helps to perform recovery and data restorations to check the time availability of recovery.

4. Deployment Team

➔ This team sends patches in phases are per the availability of downtime with its priority and criticality of the device or systems.

➔ Once patches are deployed same will be updates to inventory team, so the status of updates are updated.

5. IT and Vendor Support Team

→ With the support of IT and vendor team, they can confirm the final update status on user's workstation and respective teams will confirm their devices update status after patch deployment.

6. Network Team

→ Network team supports with the connections with respective devices, it also helps to perform shifting of traffic flow and connections from primary to secondary, DC to DR and so on.

7. Mailing Team

→ Sends notification to the teams or respective users before performing the patches or updates, and once the activity is performed. It again sends the notification to the users and team to communicate the completion of the activity.

Key Milestones

Milestones are measured on different levels at different phases.

Level 1:

- ➔ Collecting correct information of how many devices are updates and how many more devices or systems are to be done.

Level 2:

- ➔ Hardware updates or firmware updates are performed in a particular downtime, each activity is done separately in separate time frame with multiple team coordination’s including vendors availability to perform the activity.

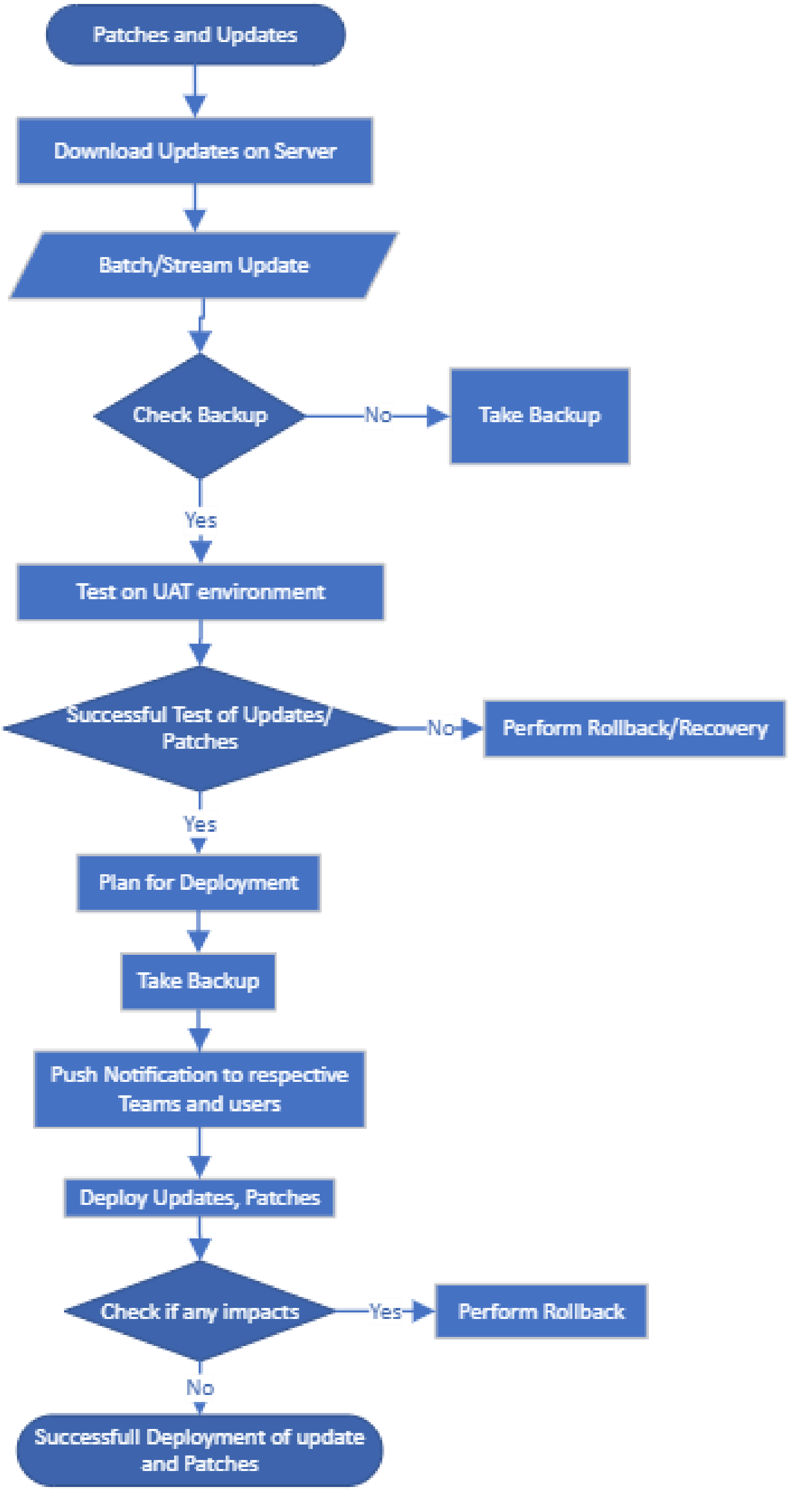
Level 3:

- ➔ Successfully completing user’s workstations and user devices updates. Once users systems are updates and compatibility are checked, new product updates can be deployed such as Microsoft exchange, antivirus updates, new drivers, printer compatibilities.

Level 4:

- ➔ This is final milestone on which user’s and team members finalize the confirmation after the patches are installed in which performance, reliability, stability are not compromised.

Flowchart of Patch Deployment



Plan notification schedule

Sending notifications to the impacted users or teams is a part of communication with helps in simplifying the process of patch deployment and bring everyone on the same page.

Notifications can be sent or communicated in various types such as Mail, Push notification (on mobile), SMS alerts and so on.

Notifications are sent Before update, after update and while performing the patch update.

Initial before update notifications is sent 1 week before the activity is performed.

While performing patch, this notification is sent by mail, or by other means of communication, in-case system is down.

After Patch update notification are the notification which confirms the completion of the activity and provides communication details if any issue faced after the patches applied.

It also provides the summary of new patch applied on the system with its performance, reliability, security and stability.

Tools available to manage patch deployments

"

1. NinjaOne
2. Automox
3. Action1
4. Atera
5. vRx
6. Pulseway" (Capterra, n.a.)

Detail breakdown of the problem

Patches are installed to overcome the performance issue, currently outdated software or the running version of the software on server or user system, patches are also used to increase the reliability, security and performance of the device, system, hardware or software.

Why install patches and what are patches?

“What are patches?

Patches are upgrades for operating systems (OS) and software that fix security flaws in a product or program. Software providers may decide to include improved security features together with performance issue fixes in updates.

How can you find which software updates you require installing?

Software providers typically post updates to their websites for users to download when they become available. To defend your phone, computer, or other digital device against hackers who would exploit system flaws, install updates at earliest. Even years or months after patches become available, attackers may continue to focus on vulnerabilities.

Various suppliers provide clients with the choice to receive updates automatically, and some software will look for updates automatically. If automatic choices are available, make sure to check with vendor's for updates on a regular basis.

Ensure that the software updates downloaded come from trusted vendor. Approve automated updates only from reliable network locations (work, home, etc.). Use a Virtual Private Network connection to a trusted network and apply updates if updates need to be installed over an trusted network.

What is the difference between manual and automatic updates?

Users can install updates manually or elect for their software programs to update automatically.

- Manual updates require the user or administrator to visit the vendor's website to download and install software files.

- Automatic updates require user or administrator consent when installing or configuring the software. Once you consent to automatic updates, software updates are "pushed" (or installed) to your system automatically.

It is recommended that users and administrators should retire all EOL products.

Best Practices for Software Updates

- Enable automatic software updates whenever possible. This will ensure that software updates are installed as quickly as possible.
- Avoid software updates on production environments.

New vulnerabilities are continually emerging, but the best defense against attackers exploiting patched vulnerabilities is simple: keep your software up to date with latest patches. This is the most effective measure you can take to protect computer, phone, and other digital devices in an organization." (*Understanding Patches and Software Updates | CISA*, 2023)

Explaining the software impacts for application patches, and end-user patches

Disadvantages of software patches

If patches are not compatible with the device or systems, it hampers the operations and impacts the users and other connected devices to it.

The moment software or application is impacted by patch it becomes unusable, and instant rollback is to be performed to make it normal as before without any data loss.

Sometimes software patches makes it incompatible with other devices or it does not support older versions running on the devices.

For example1, MS exchange

It is used to handle mail communications of users and teams and so on.

If mails communications are down, then the users will be left with no task and will not be able to communicate within the organisation.

Example2, Antivirus software

If new patch is applied and antivirus goes down, then all the users and devices become the vulnerable to attacks and huge data loss is at risk.

“Software updates are to reduce security flaws

Old software is full of security flaws. Over time, hackers find new ways to break through what was, at one time, the best available protection. Once these cybercriminals break into a system, they can spy on your computer, implant dangerous malware, or even use what they find in your system to commit identity theft.

Software updates are there to patch zero-day exploits and update older, less effective protocols to the newer, tougher-to-crack standards. This makes updating all your software one of the most critical ways to improve your computer and mobile security.

Software updates help to protect data

Data is at risk of being stolen, sold, and used against you by criminals. But the risk of being hit by a data breach is much higher if you’re using outdated software, as is the risk of accidentally destroying or corrupting your files.

Updating your software to the latest versions can close off any vulnerabilities that let hackers in. Updates can also correct problems that could corrupt your files while making sure they’re compatible with the newest versions of the programs you use.

Software updates to improve performance

If you want to make your computer faster, one of the easiest ways is to update your software. Older software versions operate using legacy code and protocols, but engineers are constantly making tweaks to improve performance and reduce resource usage. With more RAM available, your devices can do more—and do it quicker.

Reliably high performance is vital for running multiple programs simultaneously, watching high-definition videos, playing the newest games, taking the best pictures and videos, and even browsing the internet.

Software updates help protect others

The internet is a giant, interconnected network of devices. Because of the links between systems all over the globe, keeping your devices updated and free of malware and viruses that spread through networks is like covering your mouth when you cough in public." (Farrier, 2024)

Explanation on overcoming the software impacts for hardware patches

The only way to over come the software impacts after hardware patches are rolling back the updates and then finding out the solution with its vendor or the respective team. Some rollbacks are required to be performed on the moment impact is faced, there cannot be delay in waiting for downtime.

For example, if network device fails it becomes a major impact the work comes are standstill due to unavailability of network connections and internet and other resources.

Explanation of back-up and recovery requirements for all patched systems

Before performing any patch, backup is important step to perform and save minimum 2 copies at different locations to avoid any kind of data failure.

Backup consumes space but it assures data recover in the case of failures if patch is not compatible with the device or systems.

References

1. Automated Patch Management Tools Software | (Capterra, n.a.) https://www.capterra.com/sem-compare/patch-management-software/?utm_source=ps-google&utm_medium=ppc&utm_campaign=:1:CAP:2:COM:3:All:4:INTL:5:BAU:6:SOF:7:Desktop:8:BR:9:Patch_Management&network=g&gclid=CjwKCAjw9p24BhB_EiwA8ID5Bijrknxug7yKBnTV1fy8j9pxq8vkU2kf3LmQwkgYkc_V4wSwKb8KQhoCVusQAvD_BwE
2. *Understanding patches and software updates | CISA*. (2023, February 23). Cybersecurity and Infrastructure Security Agency CISA. https://www.cisa.gov/news-events/news/understanding-patches-and-software-updates
3. Farrier, E. (2024, July 26). *Why you should install software updates and operating system updates today*. https://us.norton.com/blog/how-to/the-importance-of-general-software-updates-and-patches#:~:text=Updating%20your%20software%20to%20the,of%20the%20programs%20you%20use.

Conclusion

Performing patch deployment at regular intervals is an important task which needs to be performed by every respective administrator of the organization. There are wide range of tools are available in market to manage the patches and handle the patches with monitoring features with patch updates status done or in progress of it. Semi-Automated patch system helps to reduce the administrative workload of updating the and refreshing the update status. Every organization currently in the work is dealing with some or the other way of patch deployment strategies and the ways to update the hardware, software, systems and so on. Patch deployment can be done as per organization policy such as 15 days once, monthly or quarterly as it requires frequent downtimes with is not always permissible. Patches can be deployed in different phases such as critical and noncritical patches. Few patches required vendor support for variety of devices for other expertise.