



Best practices for retiring applications before decommissioning infrastructure

AWS Prescriptive Guidance



AWS Prescriptive Guidance: Best practices for retiring applications before decommissioning infrastructure

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon's trademarks and trade dress may not be used in connection with any product or service that is not Amazon's, in any manner that is likely to cause confusion among customers, or in any manner that disparages or discredits Amazon. All other trademarks not owned by Amazon are the property of their respective owners, who may or may not be affiliated with, connected to, or sponsored by Amazon.

Table of Contents

Introduction	1
Overview	1
Targeted business outcomes	3
Best practices	4
Capture dependencies	4
Communicate your decommissioning plan to stakeholders	5
Shut down applications in a controlled manner	5
Preserve settings and data when you uninstall applications	6
Follow change management processes	6
Disconnect operational tools	7
Update asset information	8
Perform license management	8
Remove network assets	9
Remove associated databases	9
Remove associated storage devices	10
Remove associated backups	10
Use a consistent handover process for removals	11
FAQ	12
Why should I have a methodical process for decommissioning assets?	12
What happens if I switch off an application without notifying anyone?	12
How can an effective decommissioning process help me realize the business value of a cloud migration?	12
Resources	14
References	14
Tools	14
Document history	15

Best practices for retiring applications before decommissioning infrastructure

Ben Tailor-Hamblin, Amazon Web Services

Overview

The process of retiring applications and assets from infrastructure hardware before decommissioning that infrastructure is important for several reasons. First, this process ensures that any data or information that's associated with the applications and assets is properly migrated and preserved, rather than being lost when the hardware is decommissioned. This is especially important for mission-critical or sensitive data. Additionally, retiring applications and assets from your hardware can minimize or eliminate migration disruptions and downtime, so that you can more efficiently and effectively transition to the cloud. Finally, you can help your organization realize the business value of its cloud migration by retiring applications and assets. This reduces the overall cost of the migration process by eliminating the need to maintain and support unused hardware.

This guide is intended for application owners, data architects, and other roles that participate in cloud migrations or retire applications and assets from organizational infrastructure.

This guide offers recommended best practices for the following decommissioning activities:

1. Capture dependencies
2. Communicate your decommissioning plan to stakeholders
3. Shut down applications in a controlled manner
4. Preserve settings and data when you uninstall applications
5. Follow change management processes
6. Disconnect operational tools
7. Update asset information
8. Perform license management
9. Remove network assets
10. Remove associated databases
11. Remove associated storage devices

12 Remove associated backups

13 Use a consistent handover process for removals

Targeted business outcomes

The best practices covered in this guide can help you and your organization achieve the following business objectives:

- Improve efficiency by implementing the retirement and decommissioning process in a consistent, orderly way that saves time and reduces the potential for errors or complications.
- Increase cost savings by reducing the costs associated with maintaining and supporting obsolete or underutilized hardware and infrastructure.
- Minimize the risk of data loss or security breaches and protect your organization from potential liabilities and reputation damage.

Best practices

Capture dependencies

Capturing dependencies during decommissioning is important because it helps you identify and document the relationships between different systems, applications, and assets. This information is crucial for putting in place an effective decommissioning process that the decommissioning team can use to properly plan and carry out decommissioning activities without disrupting business operations. By capturing dependencies, the decommissioning team can identify any potential impacts on other systems or applications, and then take steps to address these impacts before decommissioning the relevant hardware or infrastructure. Additionally, capturing dependencies can help you identify potential cost savings or efficiencies that can be gained by decommissioning certain assets and potential risks or issues that can arise during the decommissioning process.

We recommend the following process for capturing dependencies:

1. Capture detailed dependency information for your databases, storage, network, software, and instances.
2. Obtain application owner information and confirm that this information is updated so that the decommissioning team knows who to engage with.
3. Confirm that financial and billing information for the existing application is accurate so that finance teams can forecast savings for business units.
4. Obtain details of all the hardware hosting all the application virtual machines (VMs) in all environments so that you can identify any redundant hardware that's ready for decommissioning.
5. Identify any active system communications with the application by using discovery or network monitoring tools so that dependencies can be checked.
6. Identify all underlying physical hardware running the VMs so that you can release the hardware after the decommissioning process is complete, if no other applications are using that hardware.
7. Obtain reports from teams managing the VMs to identify historic hardware usage so that you can identify VMs moving between physical hosts.
8. Perform checks to identify any replicated partner VMs so that you can include the VMs in the decommissioning process.

Communicate your decommissioning plan to stakeholders

We recommend that you communicate your decommissioning plan to stakeholders in your organization for several reasons. First, the stakeholders get the information they need to prepare for any potential disruptions or changes to their operations that may result from the decommissioning process. This can help to minimize any negative impacts on the organization and ensure that the decommissioning process is carried out in a transparent and predictable way. Additionally, communicating the decommissioning plan to stakeholders can help to generate support and buy-in for the process, which can be crucial for ensuring its success. This is especially important if the decommissioning process is likely to result in significant changes or impacts to the organization. Finally, communicating the decommissioning plan can also ensure that the process is carried out in accordance with any relevant regulations or compliance requirements. This can protect your organization from potential liabilities.

We recommend that you share your decommissioning plan with the following stakeholders:

- Application owners
- Business users
- Any teams managing downstream dependent applications or services
- Operational teams

Shut down applications in a controlled manner

Shutting down applications in a controlled manner when decommissioning the applications helps to ensure that the decommissioning process is carried out in a way that minimizes any disruptions or downtime. This is especially important for mission-critical or heavily-used applications. The decommissioning team can use a controlled shutdown process to ensure a smooth transition to alternative systems or applications, if necessary. Additionally, shutting down applications in a controlled manner can help to ensure that any data or information associated with the applications is properly preserved and migrated, rather than being lost during the decommissioning process. This can help to reduce the risk of data loss or security breaches and protect your organization from potential liabilities.

We recommend the following process for shutting down applications in a controlled manner:

1. Decouple applications from upstream and downstream services so that dependencies are removed.

2. Shut down the application so that decommissioning can proceed.
3. Remove any service schedules and shut down any crons so that the application doesn't relaunch.

Preserve settings and data when you uninstall applications

We recommend that you carry out the uninstallation process in a way that preserves any necessary configuration settings or data so that the application can be easily reinstalled if necessary. We also recommend that you properly document the uninstallation process so that it can be replicated if necessary. You can follow the uninstall guide for the application or work with the application team to uninstall your application.

Follow change management processes

Following a business change management process when you decommission your assets is important because it helps to ensure that the decommissioning process is carried out in a controlled and orderly manner. If the decommissioning team follows established change management processes, they can ensure that the necessary steps are taken to properly plan and carry out the decommissioning process and to minimize any potential impacts or disruptions to the organization. Additionally, change management processes can help to ensure that the decommissioning process is properly documented and that any necessary approvals are obtained before proceeding. This can help to reduce the risk of errors or complications during the decommissioning process and protect the organization from potential liabilities. Finally, following change management processes can also help your organization meet any relevant regulations or compliance requirements.

We recommend that you include the following in your organizational change management process:

- Database
- Storage
- Network
- VMs
- Hardware

Disconnect operational tools

By disconnecting operational tools, the decommissioning team can ensure that the assets being decommissioned are no longer being monitored, managed, used, or accessed by anyone in the organization. This can help to prevent any potential conflicts or issues during the decommissioning process. You can even help to reduce the risk of data loss or security breaches by disconnecting operational tools. Finally, disconnecting operational tools can also help to reduce the overall cost of the decommissioning process by eliminating the need to maintain and support operational tools after the assets have been decommissioned.

We recommend the following process for disconnecting operational tools:

1. Remove application log monitoring from operational systems so that the application is no longer monitored.
2. Remove metrics monitoring from operational systems so that the application is no longer monitored.
3. Remove the application from event management infrastructure monitoring so that the application is no longer monitored by support teams.
4. Remove the application from patch management systems so that the application is no longer maintained by automation tools or operational teams.
5. Turn off backup management systems to avoid the costs of redundant backup storage or operational costs from errors.
6. Remove the application from change management systems so that the application isn't listed in change management systems.
7. Decouple the application from release and deployment management systems so that the application isn't listed redundantly.
8. Remove the application from configuration management systems.
9. Remove the application from security management systems.
10. Remove the application from service catalog management systems.
11. Remove the application from antivirus systems so that the application isn't redundantly maintained.
12. Disconnect the application from encryption mechanism systems so that the application is no longer maintaining a redundant connection.

Update asset information

By updating the asset information, the decommissioning team can ensure that the assets being decommissioned are properly identified and tracked. This can help to prevent any errors or complications during the process. Additionally, updating the asset information can help to ensure that the decommissioned assets are properly accounted for and that any necessary records are kept, which can be important for compliance and audit purposes. Finally, updating the asset information can also help the business maintain a clear and accurate record of decommissioned assets. This is useful for tracking savings, future planning, and decision-making.

We recommend the following process for updating asset information:

1. Before you shut down instances, notify asset managers so that they can perform ad-hoc scans of the system. They can perform these scans by using discovery tools to capture the latest accurate service information while the instances are available.
2. Notify the asset managers when the servers go offline so that they can update the asset register.
3. Notify anyone tracking the status of application migrations for tracking purposes.
4. Provide support teams with an updated application lifecycle in the configuration management database (CMDB) that's updated for the services, software instances, applications, and hardware. This can save your organization from wasting time on investigating issues related to decommissioned assets.

Perform license management

During the decommissioning process, we recommend that you perform key license management activities. First, identify any licenses that are associated with the assets being decommissioned, and then determine if you can transfer, reassign, or cancel the licenses. This can help you avoid any potential compliance issues or additional costs associated with maintaining unused licenses. Additionally, we recommend that you properly document any changes to the license configuration so that the business has an accurate record of its license usage and entitlements. This can be useful for compliance and audit purposes and future planning and decision-making. Finally, we also recommend that you update any relevant license management tools or systems to reflect the changes resulting from the decommissioning process so that your organization can accurately track and manage its licenses going forward.

We recommend the following process for managing licenses:

1. Remove licenses so that decommissioning can take place.
2. Update any central license registers, including the CMDB.
3. Notify any third parties of license releases so that any costs can be recuperated.

Remove network assets

We recommend that you carry out the network removal process in a way that preserves any necessary configuration settings or data so that the asset can be easily reconnected to the network if necessary. It's also important to properly document the removal process so that it can be replicated if necessary.

We recommend the following process for removing network components:

1. Reclaim IP addresses so that IP addresses can be reused.
2. Remove DNS entries so that DNS entries are accurate.
3. Ensure that network teams remove or revoke public and private SSL certificates.
4. Remove load balancer rules to maintain security best practices and allow usage tracking.
5. Identify if any remaining traffic is using the load balancers or if the load balancers are free to be decommissioned so that you can raise decommissioning changes.

Remove associated databases

By removing the databases at the same time as removing the applications, the decommissioning team can ensure that the applications are no longer accessing or storing data in the databases. This best practice can help to prevent any potential conflicts or issues during the decommissioning process. Additionally, removing associated databases can help to ensure that any data or information associated with the applications is properly preserved and migrated, rather than being lost during the decommissioning process. This can help to reduce the risk of data loss or security breaches and protect your organization from potential liabilities. Finally, this best practice can also help to reduce the overall cost of the decommissioning process by eliminating the need to maintain and support the databases after application removal.

We recommend the following process for removing associated databases:

1. Share the decommissioning plan with database teams so that resources can be made available for decommissioning activities.

2. Archive the database so that any organizational or compliance data retention policies are met.
3. Remove any data assets from any data warehouses so that the decommissioned database data doesn't go stale and provide inaccurate data for business reporting.
4. Shut down and remove all database instances, including disaster recovery (DR) and backup instances.

Remove associated storage devices

Removing the storage devices can help to ensure that any data or information associated with the assets is properly migrated to the cloud, rather than being lost during the decommissioning process. This removal can also help to reduce the overall cost of the decommissioning process by eliminating the need to maintain and support storage devices after decommissioning the assets. This can result in cost savings so that your organization can realize the business value of its cloud migration.

We recommend the following process for removing storage components:

1. Back up storage devices so that data retention policies can be met.
2. Disconnect storage devices from the servers so that storage can be decommissioned.
3. Electronically scrub storage devices so that all data is securely removed and meets security standards.
4. Scrub network storage devices so that all data is securely removed and meets security standards.

Remove associated backups

We recommend that you remove associated backups in accordance with compliance and regulatory requirements when decommissioning assets because it helps to ensure that the decommissioning process complies with the relevant regulations. Different compliance and regulatory requirements may have specific requirements for the disposal or destruction of backups, and failing to comply with these requirements can result in penalties or other liabilities for your organization. Additionally, removing backups in accordance with compliance and regulatory requirements can also help to ensure that sensitive or confidential data is properly protected and that your organization is not at risk of potential security breaches or data loss.

We recommend that you shut down backups. This prevents backup tools from failing and adding to operational overhead.

Use a consistent handover process for removals

We recommend that you use a consistent handover process so that the infrastructure removal team knows which assets will be removed. The team must also understand any dependencies and be aware of any additional activities related to the decommissioning process. A consistent handover process can reduce the risk of errors and minimize potential complications during the process.

We recommend that you request the removal of physical hardware so that it can be decommissioned.

FAQ

Why should I have a methodical process for decommissioning assets?

First, a methodical process helps you take the necessary steps to properly retire the asset. This includes backing up data, removing the asset from any networks or systems it's connected to, and properly disposing of the asset. Second, a methodical process can help to prevent mistakes or oversights that could lead to data breaches or other security issues. Finally, having a clear process in place can help to make the decommissioning process more efficient and cost-effective.

What happens if I switch off an application without notifying anyone?

If you switch off an application without notifying anyone, it could cause a number of problems. First, if you shut down a mission-critical application without warning, you can cause major disruptions to your organization. This could result in lost productivity, missed opportunities, or other negative consequences. Second, if the application is connected to other systems or networks, shutting it down without warning could cause disruptions or even damage to those systems. Finally, if the application contains sensitive or confidential data, shutting it down without warning could put that data at risk of being accessed by unauthorized users. For these reasons, it's important to have a methodical process in place for decommissioning applications, and to notify the appropriate stakeholders before shutting them down.

How can an effective decommissioning process help me realize the business value of a cloud migration?

An effective decommissioning process can help you realize the business value of a cloud migration in several ways. First, it can help you retire on-premises assets in an orderly and efficient manner, which can help minimize downtime and avoid disruptions to the business during the migration process. Second, an effective decommissioning process can help to ensure that all necessary data is migrated to the cloud and that any remaining data is properly backed up or disposed of. That means you can take full advantage of the benefits of the cloud, such as increased scalability and

accessibility. Finally, an effective decommissioning process can help to reduce the overall costs of the migration by ensuring that you're only retiring and replacing assets that are necessary for the move to the cloud.

Resources

References

- [Best practices for assessing applications to be retired during a migration to the AWS Cloud](#) (AWS Prescriptive Guidance)
- [Mobilize your organization to accelerate large-scale migrations](#) (AWS Prescriptive Guidance)
- [Migrate with confidence](#) (AWS marketing)
- [Migrating to AWS: Best Practices and Strategies](#) (AWS Professional Services)

Tools

- [AWS Application Discovery Service](#) (AWS marketing)
- [AWS Transform MGN](#) (AWS marketing)
- [Modernize Data Archiving](#) (AWS marketing)

Document history

The following table describes significant changes to this guide.

Change	Description	Date
Initial publication	—	January 30, 2022