

CIS DigitalOcean Services Benchmark

v1.0.0 - 07-29-2025

Terms of Use

Please see the below link for our current terms of use:

<https://www.cisecurity.org/cis-securesuite/cis-securesuite-membership-terms-of-use/>

For information on referencing and/or citing CIS Benchmarks in 3rd party documentation (including using portions of Benchmark Recommendations) please contact CIS Legal (legalnotices@cisecurity.org) and request guidance on copyright usage.

NOTE: It is **NEVER** acceptable to host a CIS Benchmark in **ANY** format (PDF, etc.) on a 3rd party (non-CIS owned) site.

Table of Contents

Terms of Use	1
Table of Contents	2
Overview	4
Important Usage Information	4
Key Stakeholders	4
Apply the Correct Version of a Benchmark	5
Exceptions	5
Remediation	6
Summary	6
Target Technology Details	7
Intended Audience.....	7
Consensus Guidance	8
Typographical Conventions.....	9
Recommendation Definitions.....	10
Title.....	10
Assessment Status.....	10
Automated	10
Manual.....	10
Profile	10
Description.....	10
Rationale Statement	10
Impact Statement.....	11
Audit Procedure.....	11
Remediation Procedure.....	11
Default Value.....	11
References	11
CIS Critical Security Controls® (CIS Controls®).....	11
Additional Information.....	11
Profile Definitions	12
Acknowledgements	13
Recommendations	14
1 Introduction.....	14
1.1 CIS DigitalOcean Foundations Benchmarks	15
1.2 CIS DigitalOcean Services Benchmarks	16
2 Droplet.....	17
2.1 Ensure Backups are Enabled (Manual)	18

2.2 Ensure a Firewall is Created (Automated).....	32
2.3 Ensure the Droplet is Connected to a Firewall (Automated)	40
2.4 Ensure Operating System on Droplet is Upgraded (Manual)	44
2.5 Ensure Operating System is Updated (Manual)	46
2.6 Ensure Auditd is Enabled (Automated).....	48
2.7 Ensure SSH Keys are Used to Authenticate (Automated)	52
2.8 Ensure Unused SSH Keys are Deleted (Automated).....	56
3 Kubernetes.....	59
3.1 Ensure Log Forwarding is Enabled (Manual)	60
3.2 Ensure an Upgrade Window is Defined (Automated).....	63
3.3 Ensure High Availability Control Plane is Enabled (Automated)	70
4 Logging and Monitoring	74
4.1 Ensure Security History is Monitored (Manual)	75
4.2 Ensure Resource Monitoring is Enabled (Automated)	77
5 Spaces.....	80
5.1 Ensure Access Control to Spaces are Set (Manual)	81
5.2 Ensure Access and Secret Keys are Created (Manual)	83
5.3 Ensure Spaces Bucket Lifecycle Policy is Set (Automated).....	86
5.4 Ensure File Listing Permissions are Set (Manual).....	89
5.5 Ensure Spaces CDN is Enabled (Manual)	92
5.6 Ensure CORS is Enabled (Manual).....	94
5.7 Ensure Unneeded Spaces Bucket are Destroyed (Manual).....	97
6 Volumes	99
6.1 Ensure Drive is Encrypted with LUKS on Top of Volume (Manual)	100
<i>Appendix: Summary Table</i>	<i>107</i>
<i>Appendix: CIS Controls v7 IG 1 Mapped Recommendations</i>	<i>109</i>
<i>Appendix: CIS Controls v7 IG 2 Mapped Recommendations</i>	<i>110</i>
<i>Appendix: CIS Controls v7 IG 3 Mapped Recommendations</i>	<i>111</i>
<i>Appendix: CIS Controls v7 Unmapped Recommendations.....</i>	<i>112</i>
<i>Appendix: CIS Controls v8 IG 1 Mapped Recommendations</i>	<i>113</i>
<i>Appendix: CIS Controls v8 IG 2 Mapped Recommendations</i>	<i>114</i>
<i>Appendix: CIS Controls v8 IG 3 Mapped Recommendations</i>	<i>115</i>
<i>Appendix: CIS Controls v8 Unmapped Recommendations.....</i>	<i>116</i>
<i>Appendix: Change History</i>	<i>117</i>

Overview

All CIS Benchmarks™ (Benchmarks) focus on technical configuration settings used to maintain and/or increase the security of the addressed technology, and they should be used in **conjunction** with other essential cyber hygiene tasks like:

- Monitoring the base operating system and applications for vulnerabilities and quickly updating with the latest security patches.
- End-point protection (Antivirus software, Endpoint Detection and Response (EDR), etc.).
- Logging and monitoring user and system activity.

In the end, the Benchmarks are designed to be a key **component** of a comprehensive cybersecurity program.

Important Usage Information

All Benchmarks are available free for non-commercial use from the [CIS Website](#). They can be used to manually assess and remediate systems and applications. In lieu of manual assessment and remediation, there are several tools available to assist with assessment:

- [CIS Configuration Assessment Tool \(CIS-CAT® Pro Assessor\)](#)
- [CIS Benchmarks™ Certified 3rd Party Tooling](#)

These tools make the hardening process much more scalable for large numbers of systems and applications.

NOTE: Some tooling focuses only on the Benchmark Recommendations that can be fully automated (skipping ones marked **Manual**). It is important that **ALL** Recommendations (**Automated** and **Manual**) be addressed since all are important for properly securing systems and are typically in scope for audits.

Key Stakeholders

Cybersecurity is a collaborative effort, and cross functional cooperation is imperative within an organization to discuss, test, and deploy Benchmarks in an effective and efficient way. The Benchmarks are developed to be best practice configuration guidelines applicable to a wide range of use cases. In some organizations, exceptions to specific Recommendations will be needed, and this team should work to prioritize the problematic Recommendations based on several factors like risk, time, cost, and labor. These exceptions should be properly categorized and documented for auditing purposes.

Apply the Correct Version of a Benchmark

Benchmarks are developed and tested for a specific set of products and versions and applying an incorrect Benchmark to a system can cause the resulting pass/fail score to be incorrect. This is due to the assessment of settings that do not apply to the target systems. To assure the correct Benchmark is being assessed:

- **Deploy the Benchmark applicable to the way settings are managed in the environment:** An example of this is the Microsoft Windows family of Benchmarks, which have separate Benchmarks for Group Policy, Intune, and Stand-alone systems based upon how system management is deployed. Applying the wrong Benchmark in this case will give invalid results.
- **Use the most recent version of a Benchmark:** This is true for all Benchmarks, but especially true for cloud technologies. Cloud technologies change frequently and using an older version of a Benchmark may have invalid methods for auditing and remediation.

Exceptions

The guidance items in the Benchmarks are called recommendations and not requirements, and exceptions to some of them are expected and acceptable. The Benchmarks strive to be a secure baseline, or starting point, for a specific technology, with known issues identified during Benchmark development are documented in the Impact section of each Recommendation. In addition, organizational, system specific requirements, or local site policy may require changes as well, or an exception to a Recommendation or group of Recommendations (e.g. A Benchmark could Recommend that a Web server not be installed on the system, but if a system's primary purpose is to function as a Webserver, there should be a documented exception to this Recommendation for that specific server).

In the end, exceptions to some Benchmark Recommendations are common and acceptable, and should be handled as follows:

- The reasons for the exception should be reviewed cross-functionally and be well documented for audit purposes.
- A plan should be developed for mitigating, or eliminating, the exception in the future, if applicable.
- If the organization decides to accept the risk of this exception (not work toward mitigation or elimination), this should be documented for audit purposes.

It is the responsibility of the organization to determine their overall security policy, and which settings are applicable to their unique needs based on the overall risk profile for the organization.

Remediation

CIS has developed [Build Kits](#) for many technologies to assist in the automation of hardening systems. Build Kits are designed to correspond to Benchmark's "Remediation" section, which provides the manual remediation steps necessary to make that Recommendation compliant to the Benchmark.

When remediating systems (changing configuration settings on deployed systems as per the Benchmark's Recommendations), please approach this with caution and test thoroughly.

The following is a reasonable remediation approach to follow:

- CIS Build Kits, or internally developed remediation methods should never be applied to production systems without proper testing.
- Proper testing consists of the following:
 - Understand the configuration (including installed applications) of the targeted systems. Various parts of the organization may need different configurations (e.g., software developers vs standard office workers).
 - Read the Impact section of the given Recommendation to help determine if there might be an issue with the targeted systems.
 - Test the configuration changes with representative lab system(s). If issues arise during testing, they can be resolved prior to deploying to any production systems.
 - When testing is complete, initially deploy to a small sub-set of production systems and monitor closely for issues. If there are issues, they can be resolved prior to deploying more broadly.
 - When the initial deployment above is completed successfully, iteratively deploy to additional systems and monitor closely for issues. Repeat this process until the full deployment is complete.

Summary

Using the Benchmarks Certified tools, working as a team with key stakeholders, being selective with exceptions, and being careful with remediation deployment, it is possible to harden large numbers of deployed systems in a cost effective, efficient, and safe manner.

NOTE: As previously stated, the PDF versions of the CIS Benchmarks™ are available for free, non-commercial use on the [CIS Website](#). All other formats of the CIS Benchmarks™ (MS Word, Excel, and [Build Kits](#)) are available for CIS [SecureSuite®](#) members.

CIS-CAT® Pro is also available to CIS [SecureSuite®](#) members.

Target Technology Details

This Benchmark will provide secure configuration recommendations for elements of DigitalOcean's products. The recommendations detailed here are important security considerations when designing your infrastructure on the DigitalOcean platform. The specific DigitalOcean Services in scope for this document include:

- Droplet
- Kubernetes
- Logging and System Monitoring
- Spaces
- Volumes

To obtain the latest version of this guide, please visit <http://benchmarks.cisecurity.org>. If you have questions, comments, or have identified ways to improve this guide, please write us at BenchmarkInfo@cisecurity.org.

Intended Audience

This document is intended for system and application administrators, security specialists, auditors, help desk, platform deployment, and/or DevOps personnel who plan to develop, deploy, assess, or secure solutions using the DigitalOcean platform.

Consensus Guidance

This CIS Benchmark™ was created using a consensus review process comprised of a global community of subject matter experts. The process combines real world experience with data-based information to create technology specific guidance to assist users to secure their environments. Consensus participants provide perspective from a diverse set of backgrounds including consulting, software development, audit and compliance, security research, operations, government, and legal.

Each CIS Benchmark undergoes two phases of consensus review. The first phase occurs during initial Benchmark development. During this phase, subject matter experts convene to discuss, create, and test working drafts of the Benchmark. This discussion occurs until consensus has been reached on Benchmark recommendations. The second phase begins after the Benchmark has been published. During this phase, all feedback provided by the Internet community is reviewed by the consensus team for incorporation in the Benchmark. If you are interested in participating in the consensus process, please visit <https://workbench.cisecurity.org/>.

Typographical Conventions

The following typographical conventions are used throughout this guide:

Convention	Meaning
<code>Stylized Monospace font</code>	Used for blocks of code, command, and script examples. Text should be interpreted exactly as presented.
<code>Monospace font</code>	Used for inline code, commands, UI/Menu selections or examples. Text should be interpreted exactly as presented.
<code><Monospace font in brackets></code>	Text set in angle brackets denote a variable requiring substitution for a real value.
<i>Italic font</i>	Used to reference other relevant settings, CIS Benchmarks and/or Benchmark Communities. Also, used to denote the title of a book, article, or other publication.
Bold font	Additional information or caveats things like Notes , Warnings , or Cautions (usually just the word itself and the rest of the text normal).

Recommendation Definitions

The following defines the various components included in a CIS recommendation as applicable. If any of the components are not applicable it will be noted, or the component will not be included in the recommendation.

Title

Concise description for the recommendation's intended configuration.

Assessment Status

An assessment status is included for every recommendation. The assessment status indicates whether the given recommendation can be automated or requires manual steps to implement. Both statuses are equally important and are determined and supported as defined below:

Automated

Represents recommendations for which assessment of a technical control can be fully automated and validated to a pass/fail state. Recommendations will include the necessary information to implement automation.

Manual

Represents recommendations for which assessment of a technical control cannot be fully automated and requires all or some manual steps to validate that the configured state is set as expected. The expected state can vary depending on the environment.

Profile

A collection of recommendations for securing a technology or a supporting platform. Most benchmarks include at least a Level 1 and Level 2 Profile. Level 2 extends Level 1 recommendations and is not a standalone profile. The Profile Definitions section in the benchmark provides the definitions as they pertain to the recommendations included for the technology.

Description

Detailed information pertaining to the setting with which the recommendation is concerned. In some cases, the description will include the recommended value.

Rationale Statement

Detailed reasoning for the recommendation to provide the user a clear and concise understanding on the importance of the recommendation.

Impact Statement

Any security, functionality, or operational consequences that can result from following the recommendation.

Audit Procedure

Systematic instructions for determining if the target system complies with the recommendation.

Remediation Procedure

Systematic instructions for applying recommendations to the target system to bring it into compliance according to the recommendation.

Default Value

Default value for the given setting in this recommendation, if known. If not known, either not configured or not defined will be applied.

References

Additional documentation relative to the recommendation.

CIS Critical Security Controls® (CIS Controls®)

The mapping between a recommendation and the CIS Controls is organized by CIS Controls version, Safeguard, and Implementation Group (IG). The Benchmark in its entirety addresses the CIS Controls safeguards of (v7) "5.1 - Establish Secure Configurations" and (v8) "4.1 - Establish and Maintain a Secure Configuration Process" so individual recommendations will not be mapped to these safeguards.

Additional Information

Supplementary information that does not correspond to any other field but may be useful to the user.

Profile Definitions

The following configuration profiles are defined by this Benchmark:

- **Level 1**

Items in this profile intend to:

- be practical and prudent;
- provide security focused best practice hardening of a technology; and
- limit impact to the utility of the technology beyond acceptable means.

- **Level 2**

This profile extends the "Level 1" profile. Items in this profile exhibit one or more of the following characteristics:

- are intended for environments or use cases where security is more critical than manageability and usability
- acts as defense in depth measure
- may impact the utility or performance of the technology
- may include additional licensing, cost, or addition of third party software

Acknowledgements

This Benchmark exemplifies the great things a community of users, vendors, and subject matter experts can accomplish through consensus collaboration. The CIS community thanks the entire consensus team with special recognition to the following individuals who contributed greatly to the creation of this guide:

Author

Beatrix H

Contributor

Mike Wicks

Editor

Vasko Zdravevski

David Lopez

Heather Cannon

Tim Lisko

Recommendations

1 Introduction

This introduction section and the subsections herein provide informative articles which instruct on the use of the CIS Foundations and Service Category Benchmarks. No recommendations will be found in this section, just articles of relevant information.

Please carefully review the articles in this introductory section and orient yourself with our structured approach to Benchmarking for Cloud Service Providers (CSPs). This approach differs from other CIS Benchmarks because:

- there are too many different products/services in CSP product directories to practically cover in any one Benchmark,
- architectural and design decisions will affect the scope and relevance of recommendations, and
- there are a variety of methods for interfacing with CSP products and services.

Cloud Benchmarks - A Two-Step Approach to Securing Your Cloud Environments:

- **Step 1:** Start with Foundations Benchmarks. Apply as many recommendations as **practical** for your environment; "100%" 'compliance' is not always possible. Not all Foundations Benchmark recommendations can be applied at the same time, and not all recommendations will be relevant to your environment. Use the recommendation Profile Levels and your understanding of your unique environment architecture to determine which recommendations are in scope.
- **Step 2:** Use the Service Category Benchmarks for service-specific defense-in-depth recommendations. Apply recommendations only for the services **IN USE** in your environment. Use the recommendation Profile Levels, and your understanding of your unique environment architecture to determine which recommendations are in scope.

1.1 CIS DigitalOcean Foundations Benchmarks

The suggested approach for securing your DigitalOcean cloud environment is to start with the **latest version** of the CIS DigitalOcean Foundations Benchmark. Because CSP environments are constantly changing, previous versions of the Foundations Benchmarks should not be used. Previous releases may contain incorrect product names, outdated procedures, deprecated features, and other inaccuracies. The CIS Foundations Benchmark provides prescriptive guidance for configuring a subset of DigitalOcean Services with an emphasis on foundational, testable, and architecture agnostic settings for services.

The DigitalOcean Foundations Benchmark is what you should start with when beginning to secure your DigitalOcean environment. It is also the foundation for which all other DigitalOcean Service Category Benchmarks are built on so that as you grow your cloud presence and usage of the services offered you have the necessary guidance to securely configure your environment as it fits with your company's policy.

All CIS Benchmarks are created and maintained through consensus-based collaboration. Should you have feedback, suggested changes, or just like to get involved in the continued maintenance and development of CIS DigitalOcean Benchmarks, please register on CIS WorkBench at <https://workbench.cisecurity.org> and join the CIS DigitalOcean Benchmarks Community.

1.2 CIS DigitalOcean Services Benchmarks

After configuring your environment with the CIS DigitalOcean Foundations Benchmark, we suggest pursuing defense-in-depth and service-specific recommendations for your DigitalOcean Services by reviewing the Service Category Benchmarks. The Service Category Benchmarks are being produced with the vision that recommendations for all security-relevant products/services offered by a CSP should have a 'home,' but the Foundations Benchmarks should retain the most crucial recommendations and not be made vast, intimidating, and impractical.

The Service Category Benchmark recommendations should be applied **ONLY** for the CSP products and services that are actively **IN USE** in your environment. In each Service Category Benchmark, you may find that your environment uses none, or only a couple services from a list of many. Please review the services employed in your environment carefully to accurately scope the recommendations you apply. Failure to apply only the recommendations you need may introduce vulnerabilities, technical debt, and unnecessary expenses.

Using the DigitalOcean Product Directory (<https://www.digitalocean.com/products>) as a source of categorical grouping of these services, our vision is to produce a full set of CIS DigitalOcean Service Category Benchmarks to cover all security-relevant services. A list of planned and published Service Category Benchmarks for the DigitalOcean Community can be found on the community dashboard here: <https://workbench.cisecurity.org/communities/190>.

Your help is needed to bring this vision to life! Please consider joining our CIS DigitalOcean Community to contribute your expertise and knowledge in securing products and services from the DigitalOcean product family.

All CIS Benchmarks are created and maintained through consensus-based collaboration. Should you have feedback, suggested changes, or just like to get involved in the continued maintenance and development of CIS DigitalOcean Benchmarks, please register on CIS WorkBench at <https://workbench.cisecurity.org> and join the CIS DigitalOcean Benchmarks community.

2 Droplet

DigitalOcean Droplets are Linux-based virtual machines (VMs) that run on top of virtualized hardware. Each Droplet you create is a new server you can use, either standalone or as part of a larger, cloud-based infrastructure. Droplets have a set amount of CPU, RAM, and storage with an publicly accessible IP address (note: VPC Droplets are private, isolated networks).

Unless a customer has [brought their own image](#), Droplets are spun up with vanilla installs of one of six specific operating systems: AlmaLinux, CentOS, Debian, Fedora, Rocky Linux, and Ubuntu.

It is up to the customer to secure those instances and the following guide provides some best practices for how to do so.

There are many ways to improve security of the Droplet. Detailed hardening guides at the operating system level are not detailed here. For more information, please refer to the following communities and the latest published Benchmark:

[AlmaLinux Benchmark](#)

[CentOS Benchmark](#)

[Debian Benchmark](#)

[Fedora Benchmark](#)

[Rocky Linux Benchmark](#)

[Ubuntu Benchmark](#)

2.1 Ensure Backups are Enabled (Manual)

Profile Applicability:

- Level 2

Description:

Droplet backup is a service provided by DigitalOcean to help users protect their data by creating automatic, system-level backups of their Droplets. These backups enable users to have access to recent copies of their data, which can be crucial for disaster recovery and minimizing downtime in case of accidental deletion, system failures, or other data loss scenarios.

Rationale:

A few benefits of enabling backups for your Droplet are:

- **Data Loss Prevention:** Backups act as a safety net in case of data loss, accidental file deletion, or corruption. With a backup, you can restore your Droplet to a previous state.
- **Disaster Recovery:** In the event of a misconfiguration of your droplet, a hardware, software, or other significant error which renders your Droplet unusable, backups provide a method to minimize downtime by quickly recovering and rebuilding your system.
- **Easy Migration:** Backups make it easier to migrate your Droplet to a different data center or region within DigitalOcean's ecosystem. With a backup, you can spin up a new Droplet and load the backup into the new resource, thus replicating your server in a new location.
- **Security:** Regular backups can help mitigate the impact of security incidents, stemming from malware, system or app compromise, etc. Should your Droplet be compromised, you can restore the resource from a clean backup created prior to the infection rather than trying to clean a compromised system.

Impact:

In the event that you do not enable backups on your Droplet, the backup process is not properly configured or encounters issues during execution, you run the risk of having incomplete or corrupt backups, which can complicate data restoration.

Audit:

Using the DigitalOcean Control Panel to View Existing Backups

1. Sign in to your DigitalOcean account.
2. Select **Droplets** in the side panel.
3. Select a Droplet from the list.
4. Click **Backups** in the side panel to view all backups.

Using an API to List Backups for a Droplet

1. To retrieve any backups associated with a Droplet, send a GET request to

```
/v2/droplets/$DROPLET_ID/backups
```

2. You will get back a JSON object that has a backups key. This will be set to an array of backup objects, each of which contain the standard Droplet backup attributes.

Please review [List Backups for a Droplet](#) of the [DigitalOcean API](#) reference for more details.

Remediation:

Enable Backups during Droplet Creation

Using the Control Panel

1. Log in to the [DigitalOcean Control Panel](#), open the **Create** menu and select **Droplets**.
2. Fill out the fields following the normal [Droplet creation process](#). In the section, check **Enable automated backups**.
3. Here, you can select **Weekly Backups** or **Daily Backups**.
4. The backup window is a 4-hour window of time during which the Droplet automatically initiates a new backup. In the **Backup Window** section, use the drop-down menus to customize your Droplet's backup window by choosing a time of day and, for weekly backups, a day of the week.

Using Automation

You can enable backups during Droplet creation by setting the **backups** field to **true** when using the Droplet creation command or endpoint.

Using the DigitalOcean CLI

1. [Install doctl](#), the official DigitalOcean CLI.
2. [Create a personal access token](#) and save it for use with **doctl**.
3. Use the token to grant **doctl** access to your DigitalOcean account.

```
doctl auth init
```

4. Finally, run

```
doctl compute droplet create
```

Basic usage looks like this, but you can [read the usage docs](#) for more details:

```
doctl compute droplet create <droplet-name> --enable-backups true
```

Using the DigitalOcean API

1. [Create a personal access token](#) and save it for use with the API.
2. Send a POST request to <https://api.digitalocean.com/v2/droplets>.

Using cURL

```
curl -X POST \
  -H "Content-Type: application/json" \
  -H "Authorization: Bearer $DIGITALOCEAN_TOKEN" \
  -d '{"name":"example.com","region":"nyc3","size":"s-1vcpu-1gb","image":"ubuntu-20-04-x64","ssh_keys":[289794,"3b:16:e4:bf:8b:00:8b:b8:59:8c:a9:d3:f0:19:fa:45"],"backups":true,"ipv6":true,"monitoring":true,"tags":["env:prod","web"],"user_data":"#cloud-config\nruncmd:\n  - touch /test.txt\n","vpc_uuid":"760e09ef-dc84-11e8-981e-3cfdfeaae000"}' \
  "https://api.digitalocean.com/v2/droplets"
```

Using Go

Using [Godo](#), the official DigitalOcean API client for Go:

```

import (
    "context"
    "os"

    "github.com/digitalocean/godo"
)

func main() {
    token := os.Getenv("DIGITALOCEAN_TOKEN")

    client := godo.NewFromToken(token)
    ctx := context.TODO()

    createRequest := &godo.DropletCreateRequest{
        Name:      "example.com",
        Region:    "nyc3",
        Size:      "s-1vcpu-1gb",
        Image:     godo.DropletCreateImage{
            Slug: "ubuntu-20-04-x64",
        },
        SSHKeys: []godo.DropletCreateSSHKey{
            godo.DropletCreateSSHKey{ID: 289794},
            godo.DropletCreateSSHKey{Fingerprint:
"3b:16:e4:bf:8b:00:8b:b8:59:8c:a9:d3:f0:19:fa:45"}
        },
        Backups: true,
        IPv6: true,
        Monitoring: true,
        Tags: []string{"env:prod", "web"},
        UserData: "#cloud-config\nruncmd:\n - touch /test.txt\n",
        VPCUUID: "760e09ef-dc84-11e8-981e-3cfdfeaae000",
    }
}

```

Ruby

Using [DropletKit](#), the official DigitalOcean API client for Ruby:

```

require 'droplet_kit'
token = ENV['DIGITALOCEAN_TOKEN']
client = DropletKit::Client.new(access_token: token)

droplet = DropletKit::Droplet.new(
  name: 'example.com',
  region: 'nyc3',
  size: 's-1vcpu-1gb',
  image: 'ubuntu-20-04-x64',
  ssh_keys: [289794, "3b:16:e4:bf:8b:00:8b:b8:59:8c:a9:d3:f0:19:fa:45"],
  backups: true,
  ipv6: true,
  monitoring: true,
  tags: ["env:prod", "web"],
  user_data: "#cloud-config\nruncmd:\n - touch /test.txt\n",
  vpc_uuid: "760e09ef-dc84-11e8-981e-3cfdfeaae000",
)
client.droplets.create(droplet)

```

Python

Using [PyDo](#), the official DigitalOcean API client for Python:

```

import os
from pydo import Client

client = Client(token=os.environ.get("DIGITALOCEAN_TOKEN"))

req = {
    "name": "example.com",
    "region": "nyc3",
    "size": "s-1vcpu-1gb",
    "image": "ubuntu-20-04-x64",
    "ssh_keys": [
        289794,
        "3b:16:e4:bf:8b:00:8b:b8:59:8c:a9:d3:f0:19:fa:45"
    ],
    "backups": True,
    "ipv6": True,
    "monitoring": True,
    "tags": [
        "env:prod",
        "web"
    ],
    "user_data": "#cloud-config\nruncmd:\n  - touch /test.txt\n",
    "vpc_uuid": "760e09ef-dc84-11e8-981e-3cfdfeaae000"
}

resp = client.droplets.create(body=req)

```

Enable Backups on an Existing Droplet

Using the Control Panel

1. Log in to the [DigitalOcean Control Panel](#), select **Droplets** and click the Droplet you want to enable backups on. Then, click **Backups** in the left menu of the Droplet page.
2. If the Droplet already has backups enabled, click the Edit Settings button. If the Droplet does not already have backups enabled, click the **Setup Automated Backups** button.
3. Here, you can select **Weekly Backups** or **Daily Backups**.
4. The backup window is a 4-hour window of time during which the Droplet automatically initiates a new backup. In the **Backup Window** section, use the drop-down menus to customize your Droplet's backup window by choosing a time of day and, for weekly backups, a day of the week.
5. To confirm your changes, click **Enable Backups** or **Save Backup Settings**.

Using Automation

You can enable Droplet backups using the following **doctl** command, or by sending a request to the Droplet action endpoint and setting the **enable_backups** field to **true**.

Using the DigitalOcean CLI

1. [Install doctl](#), the official DigitalOcean CLI.

2. [Create a personal access token](#) and save it for use with **doctl**.
3. Use the token to grant **doctl** access to your DigitalOcean account.

```
doctl auth init
```

4. Finally, run
doctl compute droplet-action enable-backups
Basic usage looks like this, but you can [read the usage docs](#) for more details:

```
doctl compute droplet-action enable-backups <droplet-id> [flags]
```

The following example enables backups on a Droplet with the ID 386734086 with a backup policy flag:

```
doctl compute droplet-action enable-backups 386734086 --backup-policy-plan weekly --backup-policy-weekday SUN --backup-policy-hour 4
```

Using the DigitalOcean API

1. [Create a personal access token](#) and save it for use with the API.
2. Send a POST request to
https://api.digitalocean.com/v2/droplets/{droplet_id}/actions.

Using cURL


```
# Enable Backups
curl -X POST \
  -H "Content-Type: application/json" \
  -H "Authorization: Bearer $DIGITALOCEAN_TOKEN" \
  -d '{"type":"enable_backups"}' \
  "https://api.digitalocean.com/v2/droplets/3164450/actions"

# Disable Backups
curl -X POST \
  -H "Content-Type: application/json" \
  -H "Authorization: Bearer $DIGITALOCEAN_TOKEN" \
  -d '{"type":"disable_backups"}' \
  "https://api.digitalocean.com/v2/droplets/3164450/actions"

# Reboot a Droplet
curl -X POST \
  -H "Content-Type: application/json" \
  -H "Authorization: Bearer $DIGITALOCEAN_TOKEN" \
  -d '{"type":"reboot"}' \
  "https://api.digitalocean.com/v2/droplets/3164450/actions"

# Power cycle a Droplet
curl -X POST \
  -H "Content-Type: application/json" \
  -H "Authorization: Bearer $DIGITALOCEAN_TOKEN" \
  -d '{"type":"power_cycle"}' \
  "https://api.digitalocean.com/v2/droplets/3164450/actions"

# Shutdown and Droplet
curl -X POST \
  -H "Content-Type: application/json" \
  -H "Authorization: Bearer $DIGITALOCEAN_TOKEN" \
  -d '{"type":"shutdown"}' \
  "https://api.digitalocean.com/v2/droplets/3067649/actions"

# Power off a Droplet
curl -X POST \
  -H "Content-Type: application/json" \
  -H "Authorization: Bearer $DIGITALOCEAN_TOKEN" \
  -d '{"type":"power_off"}' \
  "https://api.digitalocean.com/v2/droplets/3164450/actions"

# Power on a Droplet
curl -X POST \
  -H "Content-Type: application/json" \
  -H "Authorization: Bearer $DIGITALOCEAN_TOKEN" \
  -d '{"type":"power_on"}' \
  "https://api.digitalocean.com/v2/droplets/3164450/actions"

# Restore a Droplet
curl -X POST \
  -H "Content-Type: application/json" \
  -H "Authorization: Bearer $DIGITALOCEAN_TOKEN" \
  -d '{"type":"restore", "image": 12389723 }' \
  "https://api.digitalocean.com/v2/droplets/3067649/actions"

# Password Reset a Droplet
```

```

curl -X POST \
  -H "Content-Type: application/json" \
  -H "Authorization: Bearer $DIGITALOCEAN_TOKEN" \
  -d '{"type":"password_reset"}' \
  "https://api.digitalocean.com/v2/droplets/3164450/actions"

# Resize a Droplet
curl -X POST \
  -H "Content-Type: application/json" \
  -H "Authorization: Bearer $DIGITALOCEAN_TOKEN" \
  -d '{"type":"resize","size":"1gb"}' \
  "https://api.digitalocean.com/v2/droplets/3164450/actions"

# Rebuild a Droplet
curl -X POST \
  -H "Content-Type: application/json" \
  -H "Authorization: Bearer $DIGITALOCEAN_TOKEN" \
  -d '{"type":"rebuild","image":"ubuntu-16-04-x64"}' \
  "https://api.digitalocean.com/v2/droplets/3164450/actions"

# Rename a Droplet
curl -X POST \
  -H "Content-Type: application/json" \
  -H "Authorization: Bearer $DIGITALOCEAN_TOKEN" \
  -d '{"type":"rename","name":"nifty-new-name"}' \
  "https://api.digitalocean.com/v2/droplets/3164450/actions"

# Change the Kernel
curl -X POST \
  -H "Content-Type: application/json" \
  -H "Authorization: Bearer $DIGITALOCEAN_TOKEN" \
  -d '{"type":"change_kernel","kernel":991}' \
  "https://api.digitalocean.com/v2/droplets/3164450/actions"

# Enable IPv6
curl -X POST \
  -H "Content-Type: application/json" \
  -H "Authorization: Bearer $DIGITALOCEAN_TOKEN" \
  -d '{"type":"enable_ipv6"}' \
  "https://api.digitalocean.com/v2/droplets/3164450/actions"

# Enable Private Networking
curl -X POST \
  -H "Content-Type: application/json" \
  -H "Authorization: Bearer $DIGITALOCEAN_TOKEN" \
  -d '{"type":"enable_private_networking"}' \
  "https://api.digitalocean.com/v2/droplets/3164450/actions"

# Snapshot a Droplet
curl -X POST \
  -H "Content-Type: application/json" \
  -H "Authorization: Bearer $DIGITALOCEAN_TOKEN" \
  -d '{"type":"snapshot","name":"Nifty New Snapshot"}' \
  "https://api.digitalocean.com/v2/droplets/3164450/actions"

# Acting on Tagged Droplets
curl -X POST \

```

```
-H "Content-Type: application/json" \  
-H "Authorization: Bearer $DIGITALOCEAN_TOKEN" \  
-d '{"type":"enable_backups"}' \  
"https://api.digitalocean.com/v2/droplets/actions?tag_name=awesome"  
  
# Retrieve a Droplet Action  
curl -X GET \  
-H "Content-Type: application/json" \  
-H "Authorization: Bearer $DIGITALOCEAN_TOKEN" \  
"https://api.digitalocean.com/v2/droplets/3164444/actions/36804807"
```

Go

Using [Godo](#), the official DigitalOcean API client for Go:

```

import (
    "context"
    "os"

    "github.com/digitalocean/godo"
)

func main() {
    token := os.Getenv("DIGITALOCEAN_TOKEN")

    client := godo.NewFromToken(token)
    ctx := context.TODO()
// Enable Backups
    action, _, err := client.DropletActions.EnableBackups(ctx, 3164450)

// Disable Backups
// action, _, err := client.DropletActions.DisableBackups(ctx, 3164450)

// Reboot a Droplet
// action, _, err := client.DropletActions.Reboot(ctx, 3164450)

// Power Cycle a Droplet
// action, _, err := client.DropletActions.PowerCycle(ctx, 3164450)

// Shutdown a Droplet
// action, _, err := client.DropletActions.Shutdown(ctx, 3067649)

// Power Off a Droplet
// action, _, err := client.DropletActions.PowerOff(ctx, 3164450)

// Power On a Droplet
// action, _, err := client.DropletActions.PowerOn(ctx, 3164450)

// Restore a Droplet
// action, _, err := client.DropletActions.Restore(ctx, 3164449, 12389723)

// Password Reset a Droplet
// action, _, err := client.DropletActions.PasswordReset(ctx, 3164450)

// Resize a Droplet
// action, _, err := client.DropletActions.Resize(ctx, 3164450, "1gb", true)

// Rebuild a Droplet
// action, _, err := client.DropletActions.RebuildByImageSlug(ctx, 3164450,
"ubuntu-16-04-x64")

// Rename a Droplet
// action, _, err := client.DropletActions.Rename(ctx, 3164450, "nifty-new-
name")

// Change the Kernel
// action, _, err := client.DropletActions.ChangeKernel(ctx, 3164450, 991)

// Enable IPv6
// action, _, err := client.DropletActions.EnableIPv6(ctx, 3164450)

// Enable Private Networking

```

```
// action, _, err := client.DropletActions.EnablePrivateNetworking(ctx,
3164450)

// Snapshot a Droplet
// action, _, err := client.DropletActions.Snapshot(ctx, 3164450, "Nifty New
Snapshot")

// Retrieve a Droplet Action
// action, _, err := client.DropletActions.Get(ctx, 3164450, 36804807)
```

Ruby

Using [DropletKit](#), the official DigitalOcean API client for Ruby:

```
require 'droplet_kit'
token = ENV['DIGITALOCEAN_TOKEN']
client = DropletKit::Client.new(access_token: token)

# Enable Backups
client.droplet_actions.enable_backups(droplet_id: 3164450)

# Disable Backups
# client.droplet_actions.disable_backups(droplet_id: 3164450)

# Reboot a Droplet
# client.droplet_actions.reboot(droplet_id: 3164450)

# Power Cycle a Droplet
# client.droplet_actions.power_cycle(droplet_id: 3164450)

# Shutdown a Droplet
# client.droplet_actions.shutdown(droplet_id: 3067649)

# Power Off a Droplet
# client.droplet_actions.power_off(droplet_id: 3164450)

# Power On a Droplet
# client.droplet_actions.power_on(droplet_id: 3164450)

# Restore a Droplet
# client.droplet_actions.restore(droplet_id: 3067649, image: 12389723)

# Password Reset a Droplet
# client.droplet_actions.password_reset(droplet_id: 3164450)

# Resize a Droplet
# client.droplet_actions.resize(droplet_id: 3164450, size: '1gb')

# Rebuild a Droplet
# client.droplet_actions.rebuild(droplet_id: 3164450, image: 'ubuntu-16-04-x64')

# Rename a Droplet
# client.droplet_actions.rename(droplet_id: 3164450, name: 'nifty-new-name')

# Change the Kernel
# client.droplet_actions.change_kernel(droplet_id: 3164450, kernel: 991)

# Enable IPv6
# client.droplet_actions.enable_ipv6(droplet_id: 3164450)

# Enable Private Networking
# client.droplet_actions.enable_private_networking(droplet_id: 3164450)

# Snapshot a Droplet
# client.droplet_actions.snapshot(droplet_id: 3164450, name: 'Nifty New Snapshot')
```

Python

Using [PyDo](#), the official DigitalOcean API client for Python:

```
import os
from pydo import Client

client = Client(token=os.environ.get("DIGITALOCEAN_TOKEN"))

# enable back ups example
req = {
    "type": "enable_backups"
}

resp = client.droplet_actions.post(droplet_id=346652, body=req)
```







Default Value:

Backups are disabled by default.

References:

1. <https://docs.digitalocean.com/products/custom-images/how-to/create-droplets/>
2. <https://workbench.cisecurity.org/benchmarks/11511>
3. <https://workbench.cisecurity.org/benchmarks/7036>
4. <https://workbench.cisecurity.org/benchmarks/18960>
5. <https://workbench.cisecurity.org/benchmarks/16763>
6. <https://workbench.cisecurity.org/benchmarks/18211>
7. <https://workbench.cisecurity.org/benchmarks/17074>
8. https://docs.digitalocean.com/reference/api/api-reference/#operation/droplets_list_backups
9. <https://docs.digitalocean.com/reference/api/api-reference/>
10. <https://docs.digitalocean.com/products/backups/how-to/enable/>
11. <https://cloud.digitalocean.com/>
12. <https://docs.digitalocean.com/reference/doctl/how-to/install/>
13. <https://docs.digitalocean.com/reference/api/create-personal-access-token/>
14. <https://docs.digitalocean.com/reference/doctl/reference/compute/droplet/create/>
15. <https://api.digitalocean.com/v2/droplets>
16. <https://github.com/digitalocean/godo>
17. https://github.com/digitalocean/droplet_kit
18. <https://github.com/digitalocean/pydo>
19. https://docs.digitalocean.com/reference/api/digitalocean/#operation/dropletActions_post

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	11.2 <u>Perform Automated Backups</u> Perform automated backups of in-scope enterprise assets. Run backups weekly, or more frequently, based on the sensitivity of the data.			
v7	10.2 <u>Perform Complete System Backups</u> Ensure that each of the organization's key systems are backed up as a complete system, through processes such as imaging, to enable the quick recovery of an entire system.			

2.2 Ensure a Firewall is Created (Automated)

Profile Applicability:

- Level 2

Description:

A firewall is a security system that monitors and controls network traffic based on a set of security rules, deciding whether to allow incoming and outgoing traffic to pass through to the systems behind the firewall. Firewalls usually sit between a trusted network and an untrusted network; oftentimes the untrusted network is the Internet. DigitalOcean Droplets, by default, sit on the public internet making firewalls especially critical (note: this does not apply to VPC droplets).

DigitalOcean offers a firewall product that you can use and we will discuss the usage of that product below. However, you can also use Linux provided firewall tooling like iptables, ufw, etc. Host-based firewalls are not covered here.

Rationale:

A few benefits of creating a firewall for your Droplet are:

- **Security:** Firewalls act as a bidirectional barrier between your server, a trusted network, and untrusted networks, such as the Internet. Firewalls filter incoming and outgoing network traffic based on a set of predefined rules, allowing only authorized connections to reach your Droplet.
- **Access Control:** Firewalls provide granular control over which services and ports are accessible from the Internet, therein reducing your server's attack surface.
- **Protection Against Common Attacks:** Firewalls can help mitigate common network-based attacks, such as Distributed Denial of Service (DDoS) attacks, port scanning, and brute force attacks. By blocking traffic, you can reduce the impact of these attacks on your server's performance and availability.
- **Compliance:** Many security regulations and compliance standards require the use of firewalls as a basic security measure.

Impact:

If firewall rules are too strict or incorrectly configured, legitimate traffic such as client requests, administrative access, or inter-service communication might be blocked, leading to service disruptions or degraded performance.

Audit:

Using the Control Panel

1. Log in to your DigitalOcean account at <https://cloud.digitalocean.com/login>.

2. In the DigitalOcean Control Panel, click on **Droplets** in the left sidebar to access your Droplets.
3. Find the Droplet you want to check for a firewall and click on its name to go to the Droplet's detail page.
4. In the Droplet detail page, click on the **Networking** tab.
5. Scroll down to the **Firewalls** section. If a firewall is configured for this Droplet, it will be listed here, along with its name and any associated rules.

Using the Command Line

1. Connect to your Droplet using SSH. You can do this using the following command, replacing **your-droplet-ip** with your Droplet's IP address and **your-ssh-key** with your SSH private key file:

```
ssh -i /path/to/your-ssh-key root@your-droplet-ip
```

2. Once logged in, you can check if a firewall is configured. Run the following commands:

```
doctl compute firewall list
doctl compute firewall list-by-droplet
```

If a firewall is enabled and has rules, you will see output similar to the following:

```
Status: active
```

To	Action	From
--	-----	----
OpenSSH	ALLOW	Anywhere
80/tcp	ALLOW	Anywhere

If no firewall is configured, the output will indicate that the firewall is inactive or not installed.

Remediation:

Create a Firewall Using the Control Panel

1. Log in to the [Control Panel](#).
2. Open the **Create** menu in the upper-right and choose **Cloud Firewalls**.
3. On the creation form, choose a name for your firewall in the **Name** field and then define at least one rule.

When you first create a cloud firewall, there are four inbound and outbound rules defined by default that allow some fundamental traffic. You can [keep, modify, or delete these rules, and create new ones](#).

- **Default Inbound Rule: SSH**
Because the compromise of a server typically begins over an inbound

connection, the default inbound connections remain entirely restricted with one exception. The suggested rule allows SSH connections on port 22 from anywhere so that users can to administer the server from a terminal.

- **Default Outbound Rules: Permit All Traffic**
Many fundamental services rely on outbound communication. Utilities like **ping** require outbound ICMP. DNS lookups, VoIP and NTP all rely on outbound UDP. Tasks like data synchronization, package list updates, web requests and email require outbound TCP connections.

Because of this, the suggested outbound rules permit all traffic to any destination on any port. These defaults make it easier to set up a new server without introducing restrictions that could block expected functionality.

4. Apply to Droplets

After configuring the firewall's rules, apply the firewall to the Droplets you want to secure using the **Apply to Droplets** field. You can also leave this field blank and assign Droplets later.

In the **Apply to Droplets** field, type the name of a Droplet or resource tag into the field. A drop-down populates with applicable resources. Choose Droplets by name, tag, or a combination of both. You can also search for Droplets by IP address. There are [limits on the number of Droplets and tags that can be added to a firewall](#), but there are no limits to the number of Droplets that can be associated with a tag. Using tags allows you to exceed the individual Droplet limit for firewalls. You can also tag a Droplet when you create it, which means you can apply firewall rules immediately. Droplets can be protected by more than one cloud firewall. When they are, a union of the rules is applied. For example, if one rule allows TCP from any source and another allows TCP from a restricted range, the union of the two means that TCP traffic is allowed from anywhere.

5. Create the Firewall

Once you've defined the firewall's rules and added Droplets to it, click **Create Firewall**.

After you've created a firewall, you can manage its rules and the resources that it protects from the Firewalls tab in the Networking section of the control panel.

Using the CLI

You can provide the **--droplet-ids** flag a list of Droplet IDs to automatically assign existing Droplets to a firewall during its creation. To retrieve a list of Droplets and their IDs, use the **doctl compute droplet list** command.

1. [Install doctl](#), the official DigitalOcean CLI.
2. [Create a personal access token](#) and save it for use with **doctl**.
3. Use the token to grant doctl access to your DigitalOcean account.

```
doctl auth init
```

4. Finally, run

```
doctl compute firewall create
```

Basic usage looks like this, but you can [read the usage docs](#) for more details:

```
doctl compute firewall create [flags]
```

The following example creates a cloud firewall named **example-firewall** that contains an inbound rule and an outbound rule and applies them to the specified Droplets:

```
doctl compute firewall create --name "example-firewall" --inbound-rules
"protocol:tcp,ports:22,droplet_id:386734086" --outbound-rules
"protocol:tcp,ports:22,address:0.0.0.0/0" --droplet-ids "386734086,391669331"
--tag-names "frontend,backend,k8s:f81d4fae-7dec-11d0-a765-00a0c91e6bf6"
```

Using the API

You can provide the **droplet_ids** field with an array of Droplet IDs to automatically assign existing Droplets to a firewall during its creation. To retrieve a list of Droplets and their IDs, use the [/v2/droplets endpoint](#).

1. [Create a personal access token](#) and save it for use with the API.
2. Send a POST request to <https://api.digitalocean.com/v2/firewalls>.

Using cURL

```
curl -X POST \
-H "Content-Type: application/json" \
-H "Authorization: Bearer $DIGITALOCEAN_TOKEN" \
-d
'{"name":"firewall","inbound_rules":[{"protocol":"tcp","ports":"80","sources":
{"load_balancer_uids": ["4de7ac8b-495b-4884-9a69-
1050c6793cd6"]}},{"protocol": "tcp","ports": "22","sources":{"tags":
["gateway"],"addresses":
["18.0.0.0/8"]}},{"outbound_rules":[{"protocol":"tcp","ports":"80","destinati
ons":{"addresses":["0.0.0.0/0","::/0"]}},{"droplet_ids":[8043964]}' \
"https://api.digitalocean.com/v2/firewalls"
```

GO

Using [Godo](#), the official DigitalOcean API client for Go:

```

import (
    "context"
    "os"

    "github.com/digitalocean/godo"
)

func main() {
    token := os.Getenv("DIGITALOCEAN_TOKEN")

    client := godo.NewFromToken(token)
    ctx := context.TODO()

    createRequest := &godo.FirewallRequest{
        Name: 'firewall',
        InboundRules: []godo.InboundRule{
            {
                Protocol: 'tcp',
                PortRange: '80',
                Sources: &godo.Sources{
                    LoadBalancerUIDs: []string{'4de7ac8b-495b-4884-9a69-
1050c6793cd6'},
                },
            },
            {
                Protocol: 'tcp',
                PortRange: '22',
                Sources: &godo.Sources{
                    Addresses: []string{'18.0.0.0/8'},
                    Tags: []string{'gateway'},
                },
            },
        },
        OutboundRules: []godo.OutboundRule{
            {
                Protocol: 'tcp',
                PortRange: '80',
                Destinations: &godo.Destinations{
                    Addresses: []string{'0.0.0.0/0', '::/0'},
                },
            },
        },
        DropletIDs: []int{8043964},
    }

    firewall, req, err := client.Firewalls.Create(ctx, createRequest)
}

```

Ruby

Using [DropletKit](#), the official DigitalOcean API client for Ruby:

```

require 'droplet_kit'
token = ENV['DIGITALOCEAN_TOKEN']
client = DropletKit::Client.new(access_token: token)

firewall = DropletKit::Firewall.new(
  name: 'firewall',
  inbound_rules: [
    DropletKit::FirewallInboundRule.new(
      protocol: 'tcp',
      ports: '80',
      sources: {
        load_balancer_uids: ['4de7ac8b-495b-4884-9a69-1050c6793cd6']
      }
    ),
    DropletKit::FirewallInboundRule.new(
      protocol: 'tcp',
      ports: '22',
      sources: {
        tags: ['gateway'],
        addresses: ['18.0.0.0/8']
      }
    )
  ],
  outbound_rules: [
    DropletKit::FirewallOutboundRule.new(
      protocol: 'tcp',
      ports: '80',
      destinations: {
        addresses: ['0.0.0.0/0', '::/0'],
      }
    )
  ],
  droplet_ids: [8043964]
)

client.firewalls.create(firewall)

```

Python

Using [PyDo](#), the official DigitalOcean API client for Python:

```

import os
from pydo import Client

client = Client(token=os.environ.get("DIGITALOCEAN_TOKEN"))

req = {
    "name": "firewall",
    "inbound_rules": [
        {
            "protocol": "tcp",
            "ports": "80",
            "sources": {
                "load_balancer_uids": [
                    "4de7ac8b-495b-4884-9a69-1050c6793cd6"
                ]
            }
        },
        {
            "protocol": "tcp",
            "ports": "22",
            "sources": {
                "tags": [
                    "gateway"
                ],
                "addresses": [
                    "18.0.0.0/8"
                ]
            }
        }
    ],
    "outbound_rules": [
        {
            "protocol": "tcp",
            "ports": "80",
            "destinations": {
                "addresses": [
                    "0.0.0.0/0",
                    "::/0"
                ]
            }
        }
    ],
    "droplet_ids": [
        8043964
    ]
}

resp = client.firewalls.create(body=req)



```

References:

1. <https://cloud.digitalocean.com/login>
2. <https://docs.digitalocean.com/products/networking/firewalls/how-to/create/>
3. <https://docs.digitalocean.com/reference/doctl/how-to/install/>
4. <https://docs.digitalocean.com/reference/api/create-personal-access-token/>

5. <https://docs.digitalocean.com/reference/doctl/reference/compute/firewall/create/>
6. https://docs.digitalocean.com/reference/api/digitalocean/#operation/droplets_list
7. https://docs.digitalocean.com/reference/api/digitalocean/#operation/firewalls_create
8. <https://github.com/digitalocean/godo>
9. https://github.com/digitalocean/droplet_kit
10. <https://github.com/digitalocean/pydo>
11. <https://cloud.digitalocean.com/>
12. <https://docs.digitalocean.com/products/networking/firewalls/how-to/configure-rules/>
13. <https://docs.digitalocean.com/products/networking/firewalls/#limits>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p>12.2 Establish and Maintain a Secure Network Architecture</p> <p>Establish and maintain a secure network architecture. A secure network architecture must address segmentation, least privilege, and availability, at a minimum.</p>			

2.3 Ensure the Droplet is Connected to a Firewall (Automated)

Profile Applicability:

- Level 1

Description:

A firewall is a security system that monitors and controls network traffic based on a set of security rules, deciding whether to allow incoming and outgoing traffic to pass through to the systems behind the firewall. Firewalls usually sit between a trusted network and an untrusted network; oftentimes the untrusted network is the Internet. DigitalOcean Droplets, by default, sit on the public internet making firewalls especially critical (note: this does not apply to VPC droplets).

DigitalOcean offers a firewall product that you can use and we will discuss the usage of that product below. However, you can also use Linux provided firewall tooling like iptables, ufw, etc. Host-based firewalls are not covered here.

Rationale:

A few benefits of connecting a firewall to your Droplet are:

- **Isolation Between Droplets:** Firewalls can enforce security policies that isolate Droplets from each other. This is crucial for preventing a compromised Droplet from affecting others or accessing data it shouldn't.
- **External Threat Protection:** Firewalls can be configured to monitor and filter incoming and outgoing traffic to and from Droplets, protecting them from external threats.

Impact:

If firewall rules are too strict or incorrectly configured, legitimate traffic such as client requests, administrative access, or inter-service communication might be blocked, leading to service disruptions or degraded performance.

Audit:

Using the Control Panel to Verify Your Droplet has a Firewall

1. Log in to your DigitalOcean account at <https://cloud.digitalocean.com/login>.
2. In the DigitalOcean Control Panel, click on **Droplets** in the sidebar to access your Droplets.
3. Find the Droplet you want to check for a firewall and click on its name to go to the Droplet's detail page.
4. In the Droplet detail page, click on the **Networking** tab.
5. Scroll down to the **Firewalls** section. If a firewall is configured for this Droplet, it will be listed here, along with its name and any associated rules.

Using the Command Line

1. Connect to your Droplet using SSH. You can do this using the following command, replacing **your-droplet-ip** with your Droplet's IP address and **your-ssh-key** with your SSH private key file:

```
ssh -i /path/to/your-ssh-key root@your-droplet-ip
```

2. Once logged in, you can run the following command:

```
doctl compute firewall list
```

If a firewall is enabled and has rules, you will see output similar to the following:

Status:Active			
-----	-----	-----	
To	Action	From	
OpenSSH	Allow	Anywhere	
80/TCP	Allow	Anywhere	

If no firewall is configured, the output will indicate that the firewall is inactive or not installed.

Remediation:

Add Droplets from a Firewall Using the Control Panel

1. Log in to the [control panel](#), choose **Networking** from the top menu, then **Firewalls**.
2. Select the firewall you want to check or modify, then navigate to its **Droplets** tab. A firewall's **Droplets** tab lists all of the Droplets protected by the firewall. Droplets added individually are shown on their own line, and Droplets added with a tag are shown below the tag.
3. To add another Droplet or tag to the firewall, use the **Add Droplets** button.

Using the CLI

The commands to add Droplets from a firewall require the Droplet's ID. To retrieve a list of Droplets and their IDs, use the command:

```
doctl compute droplet list
```

1. [Install doctl](#), the official DigitalOcean CLI.
2. [Create a personal access token](#) and save it for use with **doctl**.
3. Use the token to grant **doctl** access to your DigitalOcean account.

```
doctl auth init
```

4. Finally, run

```
doctl compute firewall add-droplets
```

Basic usage looks like this, but you can [read the usage docs](#) for more details:

```
doctl compute firewall add-droplets <firewall-id> [flags]
```

Using the API

The API calls to add and remove Droplets from a firewall require the Droplet's ID. To retrieve a list of Droplets and their IDs, use the [/v2/droplets endpoint](#).

1. [Create a personal access token](#) and save it for use with the API.
2. Send a POST request to https://api.digitalocean.com/v2/firewalls/{firewall_id}/droplets.

Using cURL

```
curl -X POST \
  -H "Content-Type: application/json" \
  -H "Authorization: Bearer $DIGITALOCEAN_TOKEN" \
  -d '{"droplet_ids":[49696269]}' \
  "https://api.digitalocean.com/v2/firewalls/bb4b2611-3d72-467b-8602-280330ecd65c/droplets"
```

Go

Using [Godo](#), the official DigitalOcean API client for Go:

```
import (
    "context"
    "os"

    "github.com/digitalocean/godo"
)

func main() {
    token := os.Getenv("DIGITALOCEAN_TOKEN")

    client := godo.NewFromToken(token)
    ctx := context.TODO()

    _, err := client.Firewalls.AddDroplets(ctx, 'bb4b2611-3d72-467b-8602-280330ecd65c', 49696269)
}
```

Ruby

Using [DropletKit](#), the official DigitalOcean API client for Ruby:

```
require 'droplet_kit'
token = ENV['DIGITALOCEAN_TOKEN']
client = DropletKit::Client.new(access_token: token)

client.firewalls.add_droplets([49696269], id: 'bb4b2611-3d72-467b-8602-280330ecd65c')
```

Python

Using [PyDo](#), the official DigitalOcean API client for Python:

```

import os
from pydo import Client



client = Client(token=os.environ.get("DIGITALOCEAN_TOKEN"))

req = {
    "droplet_ids": [
        49696269
    ]
}

resp = client.firewalls.assign_droplets(firewall_id="39fa4gz", body=req)

```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p>12.2 <u>Establish and Maintain a Secure Network Architecture</u></p> <p>Establish and maintain a secure network architecture. A secure network architecture must address segmentation, least privilege, and availability, at a minimum.</p>			

2.4 Ensure Operating System on Droplet is Upgraded (Manual)

Profile Applicability:

- Level 2

Description:

Upgrading an operating system is crucial for maintaining an efficient, secure, and compatible computing environment. The upgrades may provide enhanced security, improved performance, and access to new features. Regularly upgrading ensures that users can take full advantage of technological advancements while keeping their systems secure against evolving threats.

Rationale:

A few benefits of upgrading/patching the operating system on a Droplet are:

- **Security:** Newer versions of operating systems come with updated security patches which address vulnerabilities discovered in older versions.
- **Extended Support:** Older operating systems eventually reach their end-of-life, after which they no longer receive updates or support from the developers. Upgrading ensures continued support, which is crucial for maintaining a secure and stable server environment.
- **Improved Performance via Enhanced Resource Utilization:** Newer operating systems often have better mechanisms for resource allocation and management, which can lead to more efficient use of the Droplet's resources like CPU, RAM, and storage. Upgraded operating systems often come with enhancements in performance, including better memory management and faster processing. This can lead to more efficient running of applications and services hosted on the Droplet.

Impact:

Upgrades to any operating system carry an inherent risk of failure, data loss, or broken software configuration. Comprehensive backups and extensive testing are strongly advised.

Audit:

DigitalOcean supports a fixed set of operating systems: Ubuntu, AlmaLinux, Fedora, Debian, CentOS and Rocky Linux). The [End of Life.Date](#) project gives a good idea which versions of what operating system are going to expire.

Remediation:

Please note that the specific commands may vary depending on the Linux distribution you are using. The following instructions are for a typical Ubuntu-based system (such as Ubuntu, Debian, or a similar distribution).

1. SSH into your Droplet:

Open your terminal or SSH client and connect to your Droplet using its IP address or hostname. Replace with your Droplet's actual IP address:

```
ssh username@your-droplet-ip
```

If you are using a non-root user with sudo privileges, you can log in with that user and use **sudo** for administrative commands.

2. Check OS Version:

- Debian/Ubuntu OS:

```
lsb_release -a
```

- Fedora/CentOS/RedHat

```
cat /etc/os-release
```

```
cat /etc/redhat-release
```




- Other Linux Distributions

```
uname -a
```

References:

1. <https://endoflife.date/>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	2.2 <u>Ensure Authorized Software is Currently Supported</u> Ensure that only currently supported software is designated as authorized in the software inventory for enterprise assets. If software is unsupported, yet necessary for the fulfillment of the enterprise's mission, document an exception detailing mitigating controls and residual risk acceptance. For any unsupported software without an exception documentation, designate as unauthorized. Review the software list to verify software support at least monthly, or more frequently.			

2.5 Ensure Operating System is Updated (Manual)

Profile Applicability:

- Level 2

Description:

An operating system update, also known as a patch, improves an operating system's functionality, security, and stability without upgrading it to a new version. These updates address various issues such as security vulnerabilities, bugs, and other software flaws that could affect the performance and safety of the system.

Rationale:

Updating the operating system on a Droplet is important for:

- **Security:** Operating system updates often include patches for known vulnerabilities. By keeping your OS up to date, you reduce the risk of security breaches and potential attacks on your server.
- **Bug fixes:** Updates also include fixes for software bugs and stability improvements, which can help prevent unexpected crashes.
- **Performance:** Newer versions of the operating system may offer performance enhancements and optimizations, leading to improved server performance and responsiveness.
- **Compatibility:** Updated software is more likely to be compatible with the latest applications and services, ensuring that your Droplet can run modern software without issues.

Impact:

Improperly updating your operating system can cause several adverse effects, affecting system stability and security to the functionality of installed applications. Best practices for updating an operating system are regularly [backing up data](#), following official documentation, and testing updates in a controlled environment.

Audit:

DigitalOcean supports a fixed set of operating systems: Ubuntu, AlmaLinux, Fedora, Debian, CentOS and Rocky Linux). The [End of Life.Date](#) project gives a good idea which versions of what operating system are going to expire.

Remediation:

- AlmaLinux, Fedora, Rocky Linux

```
dnf update
dnf needs-restarting -r
```

- CentOS

```
dnf update
```

- Debian, Ubuntu

```
apt update
apt upgrade
```




or

```
apt dist-upgrade
```

References:

1. <https://www.digitalocean.com/security/security-best-practices-guide-droplet#ensure-backups-are-enabled>
2. <https://endoflife.date/>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	2.2 Ensure Authorized Software is Currently Supported Ensure that only currently supported software is designated as authorized in the software inventory for enterprise assets. If software is unsupported, yet necessary for the fulfillment of the enterprise's mission, document an exception detailing mitigating controls and residual risk acceptance. For any unsupported software without an exception documentation, designate as unauthorized. Review the software list to verify software support at least monthly, or more frequently.			

2.6 Ensure Auditd is Enabled (Automated)

Profile Applicability:

- Level 2

Description:

Auditd is a user-space component of the Linux Auditing System, mainly used for collecting and writing audit logs to the disk. It helps system administrators monitor security incidents by logging various system events like file accesses and user activities.

Auditd can be configured to track detailed system activity, facilitating the identification of patterns and anomalies that may be indicative of malicious behavior. The system's flexibility allows for the creation of custom rules tailored to the specific monitoring needs of an organization.

When the auditd service starts, it reads the audit.rules file to load its configuration. The audit.rules file contains specific rules that tell auditd what to log. These rules can specify which system calls to track, which files to watch for changes, and what types of user activity to monitor. Please refer to [Red Hat's Defining Audit Rules](#) guide to determine which rules are appropriate for your organization.

Refer to this list for audit record types: [Audit Record Types](#)

Rationale:

A few benefits of service auditing for a Droplet are:

- **Security:** Auditd produces logs that can help recreate events on your Droplet. This is a critically important part of recovery after a security incident or understanding events on your Droplet in a security lens.
- **Fault Detection:** Auditing helps in early detection of faults and errors in services. It allows you to identify and troubleshoot issues such as service crashes, failures, or unexpected behavior, preventing downtime and service disruptions.
- **Compliance:** For businesses and organizations that need to adhere to specific regulatory requirements or compliance standards, regular service auditing helps ensure that services are configured and operated in accordance with those standards.

Impact:

Auditd can have performance impacts if incorrectly configured. For example you may not want to audit all filesystem writes if you're running a database service.

Auditd can generate a large volume of logs, especially if configured to track a wide range of activities. This logging can consume considerable system resources (CPU, memory, and disk I/O), potentially affecting the performance of the Droplet, especially if it has limited resources.

The logs generated by auditd can quickly consume disk space. Without proper log rotation strategy and management, this can lead to disk space issues, affecting the Droplet's stability and performance.

When auditing, it is important to carefully configure the storage requirements for audit logs. By default, auditd will max out the log files at 5MB and retain only 4 copies of them. Older versions will be deleted. It is possible on a system that the 20 MBs of audit logs may fill up the system causing loss of audit data. While the recommendations here provide guidance, be sure to understand the context of your specific environment for audit storage requirements.

Audit:

To check if service auditing is set up on your DigitalOcean Droplet, you can follow these steps:

1. Log in to your DigitalOcean Droplet console using SSH.
2. DigitalOcean uses the auditd daemon for auditing. Refer to the Audit Procedure section of the Benchmark for your specific Linux distribution to test whether auditd is installed. We provide recommendations for the following distributions:
 - AlmaLinux
 - CentOS
 - Debian
 - Fedora
 - RockyLinux
 - Ubuntu

Remediation:

Follow the steps below to install and configure auditd for your operating system. Consult the Benchmark for your Linux distribution for detailed instructions

1. SSH into your Droplet by opening your terminal or SSH client and connecting to your Droplet using its IP address or hostname:

```
ssh username@your-droplet-ip
```

Replace username with your username, and your-droplet-ip with your Droplet's IP address.

2. Install auditd using the Remediation Procedure appropriate for your Linux distribution.
3. Ensure auditd is enabled and active. Please refer to the CIS Benchmark guide for your Linux distribution.
4. Enable auditd service at startup. Audit events need to be captured on processes that start up prior to auditd, so that potential malicious activity cannot go undetected. Please refer to the CIS Benchmark guide for your Linux distribution.
5. Ensure the audit backlog limit is sufficient. If audit=1 during boot, then the backlog will hold 64 records. If more than 64 records are created during boot, auditd records will be lost and potential malicious activity could go undetected. The recommended audit backlog limit value is 8192 or larger. Please refer to the CIS Benchmark guide for your Linux distribution.
6. Configure data retention. Once the log reaches the maximum size, it will be rotated and a new log file will be started. It is important that an appropriate size is determined for log files so that they do not impact the system and audit data is not lost. Please refer to the CIS Benchmark guide for your Linux distribution.
7. Configure and test auditd rules. The Audit system operates on a set of rules that define what is to be captured in the log files. The following types of Audit rules can be specified:
 - **Control rules:** Allow the Audit system's behavior and some of its configuration to be modified.
 - **File system rules:** Allow the auditing of access to a particular file or a directory. (Also known as file watches)
 - **System call rules:** Allow logging of system calls that any specified program makes.

Audit rules can be set on the command line using the auditctl utility (note: these rules are not persistent across reboots). They can also be set in a file ending in .rules in the `/etc/audit/audit.d/` directory. To define Audit rules that are persistent across reboots, you must either directly include them in the `/etc/audit/audit.rules` file or use the augenrules program that reads rules located in the `/etc/audit/rules.d/` directory.

Find the rule set right for your Droplet and use case. Refer to [Red Hat's Defining Audit Rules guide](#) and the CIS Benchmark for your Linux distribution.

8. Test the rules using the following command. No output implies correct syntax.

```
sudo auditctl -t < THE FILEPATH FOR YOUR AUDIT.RULES FILE
```

9. Configure logrotate. The system includes the capability of rotating log files regularly to avoid filling up the system with logs or making the logs unmanageably large. The file `/etc/logrotate.d/syslog` is the configuration file used to rotate log files created by syslog or rsyslog. By keeping the log files smaller and more manageable, a system administrator can easily archive these

files to another system and spend less time looking through inordinately large log files. Please refer to the CIS Benchmark guide for your Linux distribution.

References:

1. https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/security_guide/sec-defining_audit_rules_and_controls#sec-Defining_Audit_Rules_and_Controls_in_the_audit.rules_file
2. https://docs.redhat.com/en/documentation/red_hat_enterprise_linux/6/html/security_guide/sec-audit_record_types

2.7 Ensure SSH Keys are Used to Authenticate (Automated)

Profile Applicability:

- Level 2

Description:

SSH keys are a pair of cryptographic keys that can be used to authenticate to an SSH server as an alternative to password-based logins. SSH, which stands for Secure Shell, is a network protocol used to securely access and manage machines over an unsecured network. SSH keys offer a more secure way of logging into a server with SSH than using a password alone.

SSH keys must be added prior to Droplet set up. They cannot be retroactively added to Droplets when other keys are added. When the authorized keys are placed on a Droplet, they control access to the root account only, not named users. Access for named users must be setup individually on the Droplet operating system itself and not via DigitalOcean cloud platform.

Rationale:

Reasons why SSH key authentication is considered more secure than password authentication:

- **Strong Encryption:** SSH key pairs are typically generated using strong encryption algorithms, such as RSA or Ed25519, which are significantly more secure than passwords. Keys are stronger than passwords because of the asymmetric encryption key pair. A well generated key pair is much harder to brute force than a password.
- **No Passwords:** With SSH key authentication, there are no passwords involved in the authentication process. Passwords can be vulnerable to various attacks, including brute force attacks, phishing, and credential leaks. Since SSH keys are cryptographically secure, they are not susceptible to these types of attacks.
- **Lowers Probability of Credential Theft:** SSH keys are not easily stolen or intercepted because the private key is never transmitted over the network. Even if an attacker gains access to the server, they won't have access to your private key unless it's stored on the server (which is not recommended). In contrast, passwords are sent over the network during authentication and can be intercepted if the connection is not secure.
- **Logging and Accountability:** SSH key-based authentication allows for better auditing and accountability. When someone uses an SSH key to log in, their actions are associated with that key, making it easier to trace who did what on a server. Revocation and Rotation: If you suspect that your private key has been compromised, you can easily revoke it and generate a new one.

Impact:

SSH keys do not have an inherent expiration date like some other authentication methods. This means that old, possibly forgotten keys can remain valid indefinitely unless manually removed, potentially leading to unauthorized access if those keys are compromised. The security of SSH key authentication relies on the private key remaining confidential. If a user's private key is exposed or stolen, an attacker can gain access to all systems where the corresponding public key is authorized. This risk necessitates careful handling, protection (e.g., with a passphrase), and secure storage of private keys.

Audit:

To check if your DigitalOcean account has an SSH key associated:

1. Log into your DigitalOcean [Control Panel](#).
2. Select **Settings** in the bottom left of the panel.
3. Select the **Security** tab in the settings menu.
4. In the **SSH Keys** section, you should see a list of all the SSH keys associated with your DigitalOcean account. Each SSH key is typically identified by a name you provided when you added it. If there are SSH keys listed, it means you have SSH keys associated with your account.
5. Verify the key details by clicking on each SSH key to view its details, including the name, fingerprint, and the date it was added. This can help you confirm the existence of your SSH key.

If you do not see any SSH keys listed in this section, it means that there are no SSH keys associated with your DigitalOcean account. In that case, follow the steps outlined in the remediation.

Remediation:

Creating an SSH Key Before Droplet Creation

Open a terminal and run the following command (macOS example):

```
ssh-keygen
```

You will be prompted to save and name the key.

```
Generating public/private rsa key pair. Enter file in which to save the key  
(/Users/USER/.ssh/id_rsa):
```

Next you will be asked to create and confirm a passphrase for the key (highly recommended):

```
Enter passphrase (empty for no passphrase): Enter same passphrase again:
```

Copy the contents of the .pub file, typically **id_rsa.pub**.

```
cat ~/.ssh/id_rsa.pub
```

Next,

1. Go to the **Settings** section of your [DigitalOcean dashboard](#).
 2. Select the **Security** tab.
 3. Click the **Add SSH Key** button.
 4. Paste the public key into the **Public Key** box and name your key.
 5. Click the blue **Add SSH Key** button.
- This SSH key can be selected during the Choose Authentication Method step of Droplet creation.

For extra security on Ubuntu, Debian, and CentOS droplets, disable Password-based SSH authentication with the following steps:

1. Open up the SSH configuration file. It is typically found at one of the following locations, depending on your operating system:

```
sudo nano /etc/ssh/sshd_config  
sudo vi /etc/ssh/sshd_config
```

2. This command will open up the file within the text editor. Find the line in the file that includes PasswordAuthentication (or create the line if it doesn't exist), make sure it is not commented out with a # at the beginning of the line, and change it to no:

```
Password Authentication no
```

3. Save and close the file when you are finished.
 - In nano, use CTRL+O to save, hit ENTER to confirm the filename, then CTRL+X to exit.
 - In vi, press ESC and then :wq to write the changes to the file and quit.
4. Reload the sshd service to put these changes into effect:

```
sudo systemctl reload sshd
```

5. Before exiting your current SSH session, make a test connection in another terminal to verify you can still connect.

Password-based authentication for newly created Alma 9, Rocky 8, and Fedora Droplets has been disabled due to an incompatibility between the operating system's password authentication mechanism and DigitalOcean's provisioning system. SSH-based login will remain available.

Creating an SSH Key After Droplet Creation




Please select the link for your Linux distribution to learn how to create a key pair, authenticate keys, and disable password authentication for your server.

- [CentOS](#)
- [Debian](#)
- [Ubuntu](#)

References:

1. <https://www.digitalocean.com/community/tutorials/how-to-set-up-ssh-keys-on-centos-8>
2. <https://www.digitalocean.com/community/tutorials/how-to-set-up-ssh-keys-on-debian-11>
3. <https://www.digitalocean.com/community/tutorials/how-to-set-up-ssh-keys-on-ubuntu-22-04>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.6 Securely Manage Enterprise Assets and Software Securely manage enterprise assets and software. Example implementations include managing configuration through version-controlled-infrastructure-as-code and accessing administrative interfaces over secure network protocols, such as Secure Shell (SSH) and Hypertext Transfer Protocol Secure (HTTPS). Do not use insecure management protocols, such as Telnet (Teletype Network) and HTTP, unless operationally essential.			

2.8 Ensure Unused SSH Keys are Deleted (Automated)

Profile Applicability:

- Level 2

Description:

SSH keys are a pair of cryptographic keys that can be used to authenticate to an SSH server as an alternative to password-based logins. SSH, which stands for Secure Shell, is a network protocol used to securely access and manage machines over an unsecured network. SSH keys offer a more secure way of logging into a server with SSH than using a password alone.

Rationale:

Deleting SSH keys are important for:

- **Preventing Unauthorized Access** If an SSH key is no longer needed—such as for an employee who has left the company or a device that's been decommissioned—leaving it active could open a security vulnerability. Removing old or unused keys reduces the attack surface.
- **Audit Trails** For auditing and monitoring purposes, it's important to track who has access to what. Deleting keys of former users or devices ensures that audit logs are accurate and reflect actual access privileges.
- **Key Rotation**: Regularly deleting old keys and rotating them (changing to new ones) is part of good security hygiene. If a key becomes stale or compromised, attackers may exploit it, so keeping only current, active keys ensures better control over access.

Impact:

Deleting or rotating SSH keys is essential for maintaining strong security, but if not managed properly, it can lead to several issues. The most significant risk is losing access to servers if keys are deleted or rotated without properly configuring the new keys first. Automated processes and services that rely on SSH keys may break if they aren't updated, leading to disruptions. Additionally, if keys are deleted or rotated without proper documentation or communication, it could result in confusion or accidental removal of critical access.

Audit:

Using the Control Panel

1. Log in to your DigitalOcean Account.
2. Select **Settings**.
3. Click the **Security** tab.

4. The tab shows a table of created SSH keys. Review this table and ensure listed SSH keys are valid.

Using the Command Line

To get information about a key, send a GET request to

```
/v2/account/keys/$KEY_ID
```

or

```
/v2/account/keys/$KEY_FINGERPRINT
```

A 404 status will be returned if the key does not exist.

Remediation:

Using the Control Panel

1. Log in to your DigitalOcean Account.
2. Select **Settings**.
3. Click the **Security** tab.
4. The tab shows a table of created SSH keys. Select the three dots at the end of the row of the key you want to delete.
5. Select **Delete**.

Using the Command Line

To destroy a public SSH key that you have in your account, send a DELETE request to

```
/v2/account/keys/$KEY_ID
```

or

```
/v2/account/keys/$KEY_FINGERPRINT
```

A 204 status will be returned, indicating that the action was successful and that the response body is empty.

Please refer to the API documentation for deleting an SSH key from your account:

https://docs.digitalocean.com/reference/api/api-reference/#operation/sshKeys_delete

These methods delete the SSH key from the account and prevent it from being used on new Droplets, but it does not remove the SSH key from existing Droplets.

To ensure the security of existing assets, review each Droplet and either

- Delete the departing user's account or
- Remove keys from appropriate `authorized_keys` file and change the user account's password.

For each Droplet in your team account:

- Delete the departing user's user's account

If the system has configured `authorized_keys` in a different way, please remove them from however your system manages keys.

If it is necessary to keep the user account, please:




1. Change the password
2. Remove all appropriate entries from

```
/home/$departing_user_username/.ssh/authorized_keys
```

If your team's Droplets are using password auth you must:

1. Remove the user account all together; or
2. If the account must persist, change the password of the account to a complex string 18+ characters in length.
3. If the user had knowledge of the root password, and root logins are allowed in `/etc/ssh/sshd_config`, you must change the root password on all Droplets that have that password and sshd config.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.6 Securely Manage Enterprise Assets and Software Securely manage enterprise assets and software. Example implementations include managing configuration through version-controlled-infrastructure-as-code and accessing administrative interfaces over secure network protocols, such as Secure Shell (SSH) and Hypertext Transfer Protocol Secure (HTTPS). Do not use insecure management protocols, such as Telnet (Teletype Network) and HTTP, unless operationally essential.			

3 Kubernetes

DigitalOcean Kubernetes (DOKS) is a managed Kubernetes service. Deploy Kubernetes clusters with a fully managed control plane, high availability, autoscaling, and native integration with DigitalOcean Load Balancers and volumes. You can add node pools using shared and dedicated CPUs, and NVIDIA H100 GPUs in a single GPU or 8 GPU configuration. DOKS clusters are compatible with standard Kubernetes toolchains and the DigitalOcean API and CLI.

Kubernetes clusters require a balance of resources in both pods and nodes to maintain high availability and scalability. Please refer to the [Kubernetes Best Practices](#) article to help you avoid common disruption problems.

We recommend further hardening using [CIS Kubernetes Benchmark](#) guidelines, and tools like [Kyverno](#). Please keep in mind you cannot directly access or modify the kube-apiserver configuration in DOKS because the control plane is fully managed by DigitalOcean.

3.1 Ensure Log Forwarding is Enabled (Manual)

Profile Applicability:

- Level 1

Description:

Log forwarding allows you to transmit log data from various databases and applications to the log management provider of your choice, including OpenSearch, which is required for this recommendation.

Rationale:

As listed in our [Log Forwarding is Now Available for DOKS blog](#), some benefits to enabling log forwarding include:

- **Centralized log management:** Log forwarding allows customers to aggregate events across Kubernetes data plane into a centralized system. This makes it easier to manage and access cluster event logs across a distributed Kubernetes environment, rather than searching through individual nodes or containers for log data.
- **Improved monitoring and simplified troubleshooting:** With a centralized log management system, this feature allows you to consolidate logs from multiple sources, including DOKS, making it easier to monitor application performance and troubleshoot issues. Logs are crucial for identifying issues in Kubernetes clusters, and a centralized service helps users to pinpoint and resolve errors, performance bottlenecks, or configuration issues by providing a unified view of system activity.
- **Improved alerting:** By forwarding logs to a log management provider, customers can set up alerts for specific log patterns or errors. This allows them to proactively respond to potential problems or threats before they impact production environments, helping to ensure better reliability.
- **Optimized resource usage:** Combining Managed OpenSearch with DOKS helps to ensure that logs are processed, stored, and queried efficiently within a managed system optimized for performance. Both the combination and compatibility alone between DOKS and OpenSearch allows users to offload resource-intensive log aggregation and analysis to a specialized service (OpenSearch), which frees up Kubernetes resources for application workloads.

Impact:

Log forwarding has no adverse impacts.

Audit:

1. Log into your [DigitalOcean Control Panel](#).
2. Go to the [Kubernetes](#) section, select the cluster, and click the **Settings** tab.

Log forwarding is not enabled if no destinations are listed.





Remediation:

1. Go to the [Kubernetes section of the control panel](#), select the cluster, and click the **Settings** tab. In the **Event log forwarding** section, click **Edit**.
2. If you do not have an existing managed OpenSearch cluster, click **Create a database** to open the **Create Managed Database** screen. Choose a datacenter region, specify OpenSearch as the database engine, and other cluster settings as described in [Create OpenSearch Clusters](#).
3. After you create the managed OpenSearch cluster or want to select an existing cluster, click **Managed OpenSearch** to open the **Forward logs to Managed OpenSearch** window. Specify the following values:
 - **Destination Name**: Name for the destination. Provide a descriptive name for the destination.
 - **Select DigitalOcean OpenSearch database**: OpenSearch cluster to forward logs to. Select the cluster from the drop-down list.
 - **User**: The username you use to access the cluster. Use the default **doadmin** user or select another user from the drop-down list.
 - **Index name**: The name of the OpenSearch index to forward the **logs** to. Specify a lowercase index name or use the default value of logs. Indexes with uppercase characters in their names may not appear in the dashboard. For more information on indexes, see [OpenSearch's documentation](#).
4. Click **Add destination** to add the managed OpenSearch cluster as a log forwarding destination.
5. If you want to change the destination, click the ... menu and select **Edit destination** to open the **Edit Managed OpenSearch destination** window. Update the settings you want and click **Save Destination**.
6. To remove the log forwarding destination, click the ... menu and select **Remove**. Then, click **Remove destination** to confirm removing the destination.

References:

1. <https://docs.digitalocean.com/products/kubernetes/concepts/best-practices/>
2. <https://www.digitalocean.com/blog/log-forwarding-for-doks>
3. <https://cloud.digitalocean.com/kubernetes>
4. <https://docs.digitalocean.com/products/kubernetes/how-to/forward-logs/>
5. <https://docs.digitalocean.com/products/databases/opensearch/how-to/create/>
6. <https://docs.digitalocean.com/products/databases/opensearch/how-to/create/#create-a-database-cluster-using-the-control-panel>
7. <https://opensearch.org/docs/latest/im-plugin>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 <u>Collect Detailed Audit Logs</u> Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.			
v8	8.9 <u>Centralize Audit Logs</u> Centralize, to the extent possible, audit log collection and retention across enterprise assets.			

3.2 Ensure an Upgrade Window is Defined (Automated)

Profile Applicability:

- Level 2

Description:

You can upgrade DigitalOcean Kubernetes clusters to newer patch versions (for example, 1.20.1 to 1.20.2) as well as new minor versions (for example, 1.19.1 to 1.20.1) in the DigitalOcean Control Panel or in `doctl`, the command line interface (CLI) tool.

There are two ways to upgrade:

- **On demand.** When an upgrade becomes available for DigitalOcean Kubernetes, you can manually trigger the upgrade process. You can upgrade to a new minor version using the manual process, provided you first perform all available patch-level upgrades for your current minor version.
- **Automatically.** You can enable automatic upgrades for a cluster that happen within a maintenance window you specify. Automatic updates trigger on new patch versions of Kubernetes and new point releases of DigitalOcean Kubernetes subsystems with non-breaking updates. However, your cluster is not automatically upgraded to new minor Kubernetes versions (for example, 1.19.1 to 1.20.1).

Required Upgrades

When a required upgrade is scheduled for your cluster, a notification appears in the control panel indicating the target version and when the required upgrade is scheduled to occur. You can configure the weekday and time required upgrades occur in the Upgrade window in the Settings tab of the cluster. You can upgrade the cluster yourself before this date.

When a minor version becomes unsupported, we schedule an upgrade to the latest patch version of the next supported minor version. We notify you via email 30 days prior to the scheduled upgrade. We notify you again 7 days and the day before the upgrade starts.

DigitalOcean may schedule an upgrade to the latest patch version of the cluster's current minor version if a serious security vulnerability is identified in the version your cluster is running. We notify you at least 7 days before the upgrade, as well as the day before the upgrade starts.

DigitalOcean runs a cluster linter check before each required upgrade. A subset of the errors are included in the 30-day notice email and also appear in the control panel. If [cluster linter](#) errors are present, you must fix the issues.

The Upgrade Process

During an upgrade, the control plane (Kubernetes main) is replaced with a new control plane running the new version of Kubernetes. This process takes a few minutes, during which API access to the cluster is unavailable but workloads are not impacted.

Once the control plane is replaced, the worker nodes are replaced in a rolling fashion, one worker pool at a time. DOKS uses the following replacement process for the worker nodes:

1. Identify a number of nodes to drain.
2. Perform the following steps for each node concurrently:
 - a. Generate the list of pods running on it. This does not include DaemonSets or mirrored pods.
 - b. Mark the beginning of the drain start time as an annotation on the node. Eviction timeout is 15 minutes and drain (node deletion) timeout is 30 minutes.
 - c. Evict as many pods concurrently as the PodDisruptionBudget (PDB) policies allow. If the process hits the eviction timeout while draining a node, it switches to deleting the pods. If it hits the drain timeout while draining a node, it switches to deleting the node.
 - d. Wait a bit to allow for pod disruption budget to recover.
 - e. Repeat the above steps until all pods are drained.

As nodes are upgraded, workloads may experience downtime if there is no additional capacity to host the node's workload during the replacement. If you enable surge upgrades, then up to 10 new nodes for a given node pool are created up front before the existing nodes of that node pool start getting drained. Since everything happens concurrently, one node stalling the drain process doesn't stop the other nodes from proceeding. However, since one pool is upgraded at a time, it means that DOKS doesn't move to the next node pool until the current node pool finishes. When you enable surge upgrades, Kubernetes reschedules each worker node's workload, then replaces the node with a new node running the new version and reattaches any DigitalOcean Volumes Block Storage to the new nodes. The new worker nodes have new IP addresses.

Surge Upgrades Surge upgrades create duplicate upgraded nodes while, in parallel, draining workloads from old nodes to the new nodes and removing the old nodes. Surge upgrades create up to 10 duplicate nodes. As a result, larger cluster nodes are upgraded with at most 10 nodes at a time.

Surge upgrades are available at no additional cost and are enabled by default when you create a new Kubernetes cluster. We recommend enabling surge upgrades when upgrading an existing cluster for a faster and more stable upgrade.

To enable surge upgrades, in the **Surge upgrades** section of the **Settings** tab of your cluster, click **Edit**. Select the Enable surge upgrades option and click **Save**.

To use surge upgrades for the entire upgrade duration, your Droplet limit must be at least $n + \min(10, \text{num_nodes})$, where `num_nodes` is the number of nodes in your cluster and `n` is your current Droplet count. For example, if you have a 12-node cluster and 5 Droplets, your Droplet limit must at least be 15. You can [request a Droplet limit increase](#) at any time.

If an upgrade starts with less than the required number of Droplets or the limit is reached during the upgrade, then a partial upgrade is done using the available Droplets and the remaining upgrade happens without the surge enabled.

To minimize the disruptive impact of upgrades, for critical applications, we recommend setting [Pod Disruption Budgets](#).

Rationale:

Setting a cluster upgrade window has several benefits, including:

- **Alignment with business needs:** Businesses can align upgrade schedules with operational priorities to avoid updates during high-traffic times.
- **Improved security:** Scheduled upgrades ensure clusters are up-to-date with the latest patches and bug fixes.

Impact:

Some applications and dependencies may not be compatible with the latest upgrade. Upgrading your cluster can cause disruptions in the availability of services running in your workloads.

Any data stored on the local disks of the worker nodes are lost in the upgrade process. We recommend [using persistent volumes](#) for data storage, and not relying on local disk for anything other than temporary data

Audit:

Go to the [Kubernetes section of the control panel](#), select the cluster, and click the **Settings** tab. The **Automatically upgrade minor version patches** section will say **Disabled** if you do not have them installed.

Please visit the [How to Upgrade DOKS Clusters to New Versions](#) documentation for more information.

Remediation:

The default upgrade window is chosen by the DigitalOcean Kubernetes backend to guarantee an even workload across all maintenance windows for optimal processing. You can specify a different maintenance window in the **Settings** tab of a cluster. In the **Upgrade** window section, click **Edit** to specify a different start time. Upgrade windows are made up of two parts: a time of day and, optionally, a day of the week. For example, you can set your upgrade window to 5 AM any day of the week or to 8 PM on Mondays.

Using the Control Panel

Upgrading On Demand

To update a cluster manually, visit the **Overview** tab of the cluster in the [control panel](#). You see a **View Available Upgrade** button if there is a new version available for your cluster. Click this button to begin the upgrade process.

Once an upgrade starts, you can see its progress in the **Overview** and **Resources** tabs.

Upgrading to a New Minor Version

The on-demand process is required when upgrading your cluster to a new minor version of Kubernetes. During this process, you can run [our cluster linter](#) before upgrading. This automatically checks the cluster to ensure it's conforming to some common best practices, and links to [the fixes recommended in our documentation](#), to help mitigate issues that might affect your cluster's compatibility with the newer version of Kubernetes. Click **Run Linter** on the upgrade window to begin.

Upgrading to New Control Plane

DigitalOcean Kubernetes clusters originally created with version 1.20 or older have a version of the control plane architecture which does not allow you to enable [high availability](#). However, you can now upgrade your control plane to the new version. This upgrade option is available for Kubernetes versions currently 1.22 and later.

In the cluster's **Overview** page or the **View Available Upgrade** pop-up list, follow the upgrade process to get the new control plane.

The upgrade process may disrupt your cluster's operations for up to approximately 2 minutes. This is because the upgrade involves a significant Cilium configuration change; so, during the migration, many worker nodes are on different configurations and therefore cannot communicate with each other until all the pods have rapidly restarted.

In addition to following the steps to [minimize disruptions during upgrades](#), we recommend you do not create any new workloads during the upgrade. This includes creating new deployments and increasing replica count for existing processes manually or automatically (such as with replica-adjusting controllers like HPA).

Upgrading Automatically

To enable automatic upgrades for a cluster, visit the **Settings** tab of the cluster. In the **Automatically upgrade minor version patches** section, click the **Automatically install minor version patches** checkbox.

Automatic upgrades occur during a cluster's 4-hour upgrade window. The default upgrade window is chosen by the DigitalOcean Kubernetes backend to guarantee an even workload across all maintenance windows for optimal processing.

You can specify a different maintenance window in the **Settings** tab of a cluster. In the **Upgrade window** section, click **Edit** to specify a different start time. Upgrade windows are made up of two parts: a time of day and, optionally, a day of the week. For example, you can set your upgrade window to 5 AM any day of the week or to 8 PM on Mondays. You receive a notification email 30 days, 7 days, and 1 day before an automatic upgrade.

Even if you have auto upgrades enabled, you can still upgrade on-demand by clicking the **View Available Upgrade** button in the **Overview** tab.

Upgrade Using Automation

If you do not provide a **version** in the version field, the cluster upgrades to the next minor version of Kubernetes (for example, 1.28.1 to 1.29.1). You can retrieve a list of

available version using the [/v2/kubernetes/options endpoint](#) or the `doctl kubernetes options` command.

Upgrade Using the DigitalOcean CLI

1. [Install doctl](#), the official DigitalOcean CLI.
2. [Create a personal access token](#) and save it for use with `doctl`.
3. Use the token to grant `doctl` access to your DigitalOcean account.

```
doctl auth init
```

4. Finally, run `doctl kubernetes cluster upgrade`. Basic usage looks like this, but you can [read the usage docs](#) for more details:

```
doctl kubernetes cluster upgrade <id|name> [flags]
```

The following example upgrades a cluster named example-cluster to version 1.28.2:

```
doctl kubernetes cluster upgrade example-cluster --version 1.28.2-do.0
```

Upgrade Using the DigitalOcean API

1. [Create a personal access token](#) and save it for use with the API.
2. Send a POST request to https://api.digitalocean.com/v2/kubernetes/clusters/{cluster_id}/upgrade.

cURL

Using cURL:

```
curl -X GET \
  -H "Content-Type: application/json" \
  -H "Authorization: Bearer $DIGITALOCEAN_TOKEN" \
  "https://api.digitalocean.com/v2/kubernetes/clusters/bd5f5959-5e1e-4205-a714-a914373942af/upgrades"
```

Go

Using [Godo](#), the official DigitalOcean API client for Go:

```
import (
    "context"
    "os"

    "github.com/digitalocean/godo"
)

func main() {
    token := os.Getenv("DIGITALOCEAN_TOKEN")

    client := godo.NewFromToken(token)
    ctx := context.TODO()

    upgradeRequest := &godo.KubernetesClusterUpgradeRequest{
        VersionSlug: "1.12.3-do.1",
    }
}
```

Python

Using [PyDo](#), the official DigitalOcean API client for Python:

```
import os
from pydo import Client

client = Client(token=os.environ.get("DIGITALOCEAN_TOKEN"))

req = {
    "version": "1.16.13-do.0"
}

resp = client.kubernetes.upgrade_cluster(cluster_id="1fd32a", body=req)
```

Upgrading to a Specific Version

To upgrade to a specific Kubernetes version, rather than automatically upgrading to the latest version, you must first use your cluster ID to get a list of available upgrades for that cluster:

```
doctl kubernetes cluster get-upgrades <cluster-id>
```

Then, use the **slug** value returned by the **get-upgrades** call to perform the upgrade:







```
doctl kubernetes cluster upgrade <cluster-id> --version 1.20.2-do.0
```

References:

1. <https://cloud.digitalocean.com/kubernetes>
2. <https://docs.digitalocean.com/products/kubernetes/how-to/upgrade-cluster/>
3. <https://github.com/digitalocean/clusterlint>
4. <https://docs.digitalocean.com/products/kubernetes/how-to/add-volumes/>
5. <https://docs.digitalocean.com/platform/accounts/#droplet-and-volume-limit-increases>
6. <https://docs.digitalocean.com/products/kubernetes/how-to/upgrade-cluster/#disruption-free-upgrades>
7. <https://cloud.digitalocean.com/>

8. <https://docs.digitalocean.com/support/clusterlint-error-fixes/>
9. <https://docs.digitalocean.com/products/kubernetes/details/managed/#managed-elements-of-the-control-plane>
10. <https://docs.digitalocean.com/products/kubernetes/how-to/upgrade-cluster/#disruption-free-upgrades>
11. https://docs.digitalocean.com/reference/api/digitalocean/#operation/kubernetes_list_options
12. <https://docs.digitalocean.com/reference/doctl/reference/kubernetes/options/>
13. <https://docs.digitalocean.com/reference/doctl/how-to/install/>
14. <https://docs.digitalocean.com/reference/api/create-personal-access-token/>
15. <https://docs.digitalocean.com/reference/doctl/reference/kubernetes/cluster/upgrade/>
16. https://docs.digitalocean.com/reference/api/digitalocean/#operation/kubernetes_upgrade_cluster
17. <https://github.com/digitalocean/godo>
18. <https://github.com/digitalocean/pydo>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	7.3 Perform Automated Operating System Patch Management Perform operating system updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.			
v8	7.4 Perform Automated Application Patch Management Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.			

3.3 Ensure High Availability Control Plane is Enabled (Automated)

Profile Applicability:

- Level 1

Description:

DigitalOcean Kubernetes provides a [high availability \(HA\)](#) option that increases uptime and provides 99.95% SLA uptime for control planes. If you enable high availability for a cluster, multiple replicas of each control plane component are created, ensuring that a redundant replica is available when a failure occurs. This results in additional increased uptime.

Rationale:

Enabling the High Availability Control Plane increases performance and offers several benefits, including:

- **Minimized downtime:** The redundancy and failover mechanisms of high availability ensure services remain operational.
- **Improved performance:** High availability optimizes resource utilization.
- **Resiliency:** High Availability automatically detects and replaces unhealthy components and dynamically allocates CPU and memory resources on demand.

Impact:

Enabling the High Availability Control Plane offers better resilience, but may increase costs. Once enabled, you cannot disable high availability.

Audit:

Go to the [Kubernetes section of the control panel](#), and click the **Overview** tab. Scroll down to the Control Pane. The High Availability status will say **Not Enabled** or **Enabled**, depending on your settings.

Remediation:

Using the Control Panel

To enable high availability on an existing cluster, go to the [control panel](#) and click the cluster you want to enable high availability on. Then, in the **Overview** tab, scroll down and find the **Control Plane** card.

In the card, click **Add high availability**. This opens a pop-up window where you can confirm your change. Once enabled, you cannot disable high availability in the future.

DigitalOcean Kubernetes clusters originally created with version 1.20 or older have a version of the control plane which does not allow you to enable [high availability](#). If you cannot find this card, upgrade your control plane.

To check whether you can upgrade your cluster to the new control plane, see [Upgrading to New Control Plane](#).

Using Automation

You can enable high availability using the DigitalOcean Kubernetes **doctl** update command or API endpoint by setting the **ha** value to **true**.

How to Update a Kubernetes Cluster Using the DigitalOcean CLI

1. [Install doctl](#), the official DigitalOcean CLI.
2. [Create a personal access token](#) and save it for use with **doctl**.
3. Use the token to grant doctl access to your DigitalOcean account.

```
doctl auth init
```

4. Finally, run **doctl kubernetes cluster update**. Basic usage looks like this, but you can [read the usage docs](#) for more details:

```
doctl kubernetes cluster update <id|name> [flags]
```

How to Update a Kubernetes Cluster Using the DigitalOcean API

1. [Create a personal access token](#) and save it for use with the API.
2. Send a PUT request to https://api.digitalocean.com/v2/kubernetes/clusters/{cluster_id}.

cURL

Using cURL:

```
curl -X PUT \
  -H "Content-Type: application/json" \
  -H "Authorization: Bearer $DIGITALOCEAN_TOKEN" \
  -d '{"name": "stage-cluster-01", "tags":["staging", "web-team"]}' \
  "https://api.digitalocean.com/v2/kubernetes/clusters/bd5f5959-5e1e-4205-a714-a914373942af"
```

Go

Using [Godo](#), the official DigitalOcean API client for Go:


```

import (
    "context"
    "os"

    "github.com/digitalocean/godo"
)

func main() {
    token := os.Getenv("DIGITALOCEAN_TOKEN")

    client := godo.NewFromToken(token)
    ctx := context.TODO()

    updateRequest := &godo.KubernetesClusterUpdateRequest{
        Name: "stage-cluster-01",
        Tags: []string{"staging", "web-team"},
    }

    cluster, _, err := client.Kubernetes.Update(ctx, "bd5f5959-5e1e-4205-a714-a914373942af", updateRequest)
}

```

Ruby

Using [DropletKit](#), the official DigitalOcean API client for Ruby:

```

require 'droplet_kit'
token = ENV['DIGITALOCEAN_TOKEN']
client = DropletKit::Client.new(access_token: token)

cluster = DropletKit::KubernetesCluster.new(
  name: 'foo',
  tags: ['staging', 'web-team']
)

client.kubernetes_clusters.update(cluster, id: 'bd5f5959-5e1e-4205-a714-a914373942af')

```

Python

Using [PyDo](#), the official DigitalOcean API client for Python:

```

import os
from pydo import Client

client = Client(token=os.environ.get("DIGITALOCEAN_TOKEN"))

req = {
    "name": "prod-cluster-01",
    "tags": [
        "k8s",
        "k8s:bd5f5959-5e1e-4205-a714-a914373942af",
        "production",
        "web-team"
    ],
    "maintenance_policy": {
        "start_time": "12:00",
        "day": "any"
    },
    "auto_upgrade": True,
    "surge_upgrade": True,
    "ha": True
}

resp = client.kubernetes.update_cluster(cluster_id="1fd32a", body=req)

```

References:

1. <https://docs.digitalocean.com/products/kubernetes/details/managed/#managed-elements-of-the-control-plane>
2. <https://cloud.digitalocean.com/kubernetes>
3. <https://docs.digitalocean.com/products/kubernetes/how-to/enable-high-availability/>
4. <https://docs.digitalocean.com/reference/doctl/how-to/install/>
5. <https://docs.digitalocean.com/reference/api/create-personal-access-token/>
6. <https://docs.digitalocean.com/reference/doctl/reference/kubernetes/cluster/update/>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

4 Logging and Monitoring

This section contains recommendations for using DigitalOcean's Logging and Monitoring features to monitor events and gather metrics about Droplet-level resource utilization.

4.1 Ensure Security History is Monitored (Manual)

Profile Applicability:

- Level 1

Description:

The security history of your Droplet shows a record of actions that have been taken in an account. Within the history, users can find a record of actions taken within your account, such as user logins, password changes, and resource creation, augmentation, and deletion.

Each record includes the IP address of the device where the action originated and a correlative time stamp.

Rationale:

Monitoring supports the detection of unusual activities that might indicate a security breach.

Impact:

There are no adverse consequences by monitoring security history.

Audit:

As of publication date, the only way to access the security history is through the cloud UI.

1. Sign in to your [DigitalOcean dashboard](#).
2. Go to the **Settings** menu.
3. Click the **Security** tab.
4. The bottom of the page will have a table of your account's security history. It will list the action taken, the user's name, email address, and IP address, and the time the action was taken.

Remediation:

Security History can not be turned off.



Default Value:

Security History is enabled by default.

References:

1. <https://cloud.digitalocean.com/>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.11 <u>Conduct Audit Log Reviews</u> Conduct reviews of audit logs to detect anomalies or abnormal events that could indicate a potential threat. Conduct reviews on a weekly, or more frequent, basis.			

4.2 Ensure Resource Monitoring is Enabled (Automated)

Profile Applicability:

- Level 1

Description:

DigitalOcean Monitoring is a free, opt-in service that gathers metrics about Droplet-level resource utilization. It provides additional Droplet graphs and supports configurable metrics alert policies with integrated email Slack notifications to help you track the operational health of your infrastructure.

Rationale:

Resource monitoring is important for many reasons, including:

- **Real-time Insights:** Monitoring provides real-time information on utilization and performance, enabling swift responses to anomalies or outages and supporting faster diagnosis and mitigation of security-related problems to minimize downtime and reduce the window of vulnerability.
- **Performance Optimization:** By analyzing metrics such as CPU utilization and memory usage, customers can optimize their applications for better speed and responsiveness.
- **Audit Support:** Retaining monitoring data for 14 days allows security teams to review historical performance and usage patterns, facilitating forensic analysis to understand the timeline and impact of security events.

Impact:

Metrics agents typically consume system resources like CPU, memory, and network bandwidth to collect and transmit data. While usually minimal, this overhead can impact the performance of the server, especially if the server is already under heavy load or has limited resources.

Audit:

Follow these steps to ensure monitoring is activated:

1. Sign in to your [DigitalOcean account](#).
2. Select **Droplets** under the **Manage** menu.
3. Click on the name of the Droplet.
The security monitoring page will display graphs of CPU percentages, memory use, disk input/output, and other metrics.

Remediation:

Installing the Metrics Agent on a New Droplet

Using the Control Panel

To install the metrics agent during Droplet creation with the control panel, find the We recommend these options section and click Enable Monitoring. The metrics agent will be automatically installed and enabled during the Droplet creation process.

Using the API or CLI

If you are using the DigitalOcean API to create Droplets, set the **monitoring** attribute to **true** in the creation parameters to automatically install the metrics agent on the Droplet during creation. The Droplet creation section of the API documentation contains additional details.

```
{
  "name": "example.com",
  "region": "nyc3",
  "size": "s-1vcpu-1gb",
  "image": "ubuntu-20-04-x64",
  "ssh_keys": [
    289794,
    "3b:16:e4:bf:8b:00:8b:b8:59:8c:a9:d3:f0:19:fa:45"
  ],
  "backups": true,
  "ipv6": true,
  "monitoring": true,
  "tags": [
    "env:prod",
    "web"
  ],
  "user_data": "#cloud-config\nruncmd:\n  - touch /test.txt\n",
  "vpc_uuid": "760e09ef-dc84-11e8-981e-3cfdfeaae000"
}
```

If you are using **doctl**, the DigitalOcean command line client, to create Droplets with the **doctl compute droplet create** command, use the **-enable-monitoring** flag to enable monitoring.

Installing the Metrics Manually

You can also install the metrics agent manually on supported operating systems and versions. There is an installation script available that automatically detects the client operating system and configures repositories to install the agent.

Please refer to the [How to Install the DigitalOcean Metric Agent](#) guide for instructions.



Set up Resource Alerts

[Set up resource alerts](#) after installing the metrics agent to track the operational health of your infrastructure.

References:

1. <https://cloud.digitalocean.com/>
2. <https://docs.digitalocean.com/products/monitoring/how-to/install-agent/>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.11 <u>Conduct Audit Log Reviews</u> Conduct reviews of audit logs to detect anomalies or abnormal events that could indicate a potential threat. Conduct reviews on a weekly, or more frequent, basis.			

5 Spaces

Spaces Object Storage is an S3-compatible object storage service. Spaces buckets let you store and serve large amounts of data, and the built-in CDN minimizes page load times and improves performance.

This section contains recommendations for configuring DigitalOcean Spaces for improved security.

5.1 Ensure Access Control to Spaces are Set (Manual)

Profile Applicability:

- Level 2

Description:

Spaces owners can create, destroy, and read all content in all the Spaces buckets for an account. They also make decisions and manage what everyone else can see. If an owner wants to allow one or more people to co-manage buckets, there are two options: Access Keys and DigitalOcean Teams.

Access Keys

Users who connect with access keys can create, destroy, read, and write to all of the buckets for the account. However, the privileges granted by Spaces access keys do not provide access to the control panel and do not extend to other DigitalOcean resources.

DigitalOcean Teams

Teams allow members to use the control panel, including creating, managing, and destroying buckets associated with the Team account. Team members can also create, delete, and regenerate access keys for buckets.

Unlike Spaces access keys, members of a Team can also access other Team resources like Droplets, Firewalls, and more.

Rationale:

Managing access to your DigitalOcean Spaces Object Storage is important for:

-Data Security: Unauthorized access can lead to data breaches, exposure of sensitive information, and potential manipulation or deletion of critical data. **-Compliance Regulations:** Many organizations are subject to regulations such as GDPR, HIPAA, or PCI-DSS, which require strict data protection controls and protocols. **-Insider Threat Protection:** Insider threats, either malicious or accidental, can be as dangerous as external attacks. Properly managing access helps mitigate the risks posed by insiders by ensuring that individuals only have access to the data and resources necessary for their job functions.

Impact:

Misconfigured permissions can either expose sensitive data or lock users out of the data they need to perform their jobs. Frequent changes in team structures or project scopes can exacerbate these risks as updates to access controls may not keep pace.

Audit:

1. Sign into your DigitalOcean account.

2. Navigate to the **Spaces Object Storage** page.
3. Select the **Access Keys** tab.
4. Review the relationships between key permissions and buckets.
5. Review our "How to Manage Administrative Access to Spaces" guide to learn more.

Remediation:

1. Sign into your DigitalOcean account.
2. Navigate to the **Spaces Object Storage** page.
3. Select the **Access Keys** tab.
4. Review the relationships between key permissions and buckets.
5. If changes are necessary, review our [How to Manage Administrative Access to Spaces](#) guide to learn more.




Default Value:

File listings are restricted by default.

References:

1. <https://docs.digitalocean.com/products/spaces/how-to/manage-access/>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			

5.2 Ensure Access and Secret Keys are Created (Manual)

Profile Applicability:

- Level 2

Description:

DigitalOcean Spaces Object Storage uses access and secret keys to control and manage access to data. Access and secret keys are used for authentication and authorization when accessing the Spaces service.

The access key is a public identifier for your account. It is used to identify the user making the request to a Spaces bucket. The secret key is a private key associated with your access key. It should be kept confidential and secure. This key is used in conjunction with the access key to sign requests to the Spaces API, ensuring that the request is authorized.

There are two scope options for access keys:

- **Limited**, which grants access to specific buckets with read or read/write/delete permissions.
- **Full Access**, which grants unrestricted access to all supported [S3 APIs](#), including bucket creation and configuration (lifecycle, bucket policies, versioning, CORS, and website), and listing all buckets.

Rationale:

Creating access and secret keys is important for the following reasons:

- **Security**: Access and secret keys allow you to securely access your DigitalOcean Spaces. They function similarly to a username and password, ensuring that only authorized users and applications can access your data.
- **Authentication**: Access and secret keys are used to authenticate your requests to the Spaces API. Without proper authentication, your requests will be denied, preventing unauthorized access.

Impact:

While creating access and secret keys are considered a best Security practice, there are considerations to remain abreast of. For instance, if access keys are hard-coded into applications or stored insecurely, they can be exposed through source code repositories, configuration files, or logs, which increases the risk of unauthorized access. In addition, rotating or revoking keys without proper planning can lead to service disruptions. Furthermore, applications or users relying on the old keys might lose access until updated keys are deployed.

Audit:

1. Sign in to your [DigitalOcean account](#).
2. Navigate to the [Spaces Access Key](#) page.
3. Review Access Key permissions relative to their affiliated buckets and Read/Write/Delete capabilities.
4. If augmentations are necessary, follow the steps outlined in the [Description](#) or in the [Remediation Procedure](#).

Remediation:

Create Spaces Access Key

1. Sign in to your [DigitalOcean account](#).
2. Navigate to the [Spaces Object Storage](#) page.
3. Select the [Access Keys](#) tab.
4. If necessary, select [Create Access Key](#) to open the [New Spaces Access Key](#) window.
5. Select the key's access scope:
 - a. Full access: Allows all S3 API commands on all buckets
 - b. Limited access: Permits more specific Read or Read/Write/Delete permissions for each bucket.
6. If limited access was selected, check the boxes for the buckets the key should have access to. For each bucket, use the drop down menu to designate Read or Read/Write/Delete permissions.
7. Name the key and click [Create Access Key](#).
8. Immediately copy the Secret Key to a secure location as it will not be shown again.

Edit Limited Access Spaces Key Permissions




1. Sign in to your [DigitalOcean account](#).
2. Navigate to the [Spaces Access Keys](#) page.
3. Locate the key and select [More \(...\)](#).
4. Select [Edit Permissions](#) to open the [Edit Permissions](#) window.
5. Select the boxes for the buckets they key should have access to.
6. If necessary, change the permissions level via the provided dropdown.

For more information on creating and managing access to Access Keys, please visit our [How to Manage Access Keys](#) documentation.

References:

1. <https://docs.digitalocean.com/products/spaces/reference/s3-compatibility/>
2. <https://docs.digitalocean.com/products/spaces/how-to/manage-access/>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			

5.3 Ensure Spaces Bucket Lifecycle Policy is Set (Automated)

Profile Applicability:

- Level 1

Description:

A lifecycle configuration rule is a policy or rule set to manage the lifecycle of objects in a storage bucket. These rules automate the process of transitioning objects through different storage classes or deleting them after they are no longer needed. The objective is to optimize costs and manage data efficiently without manual intervention.

There are several cross-platform command-line tools available to tools for managing S3 and S3-compatible stores, but this example offers guidance on s3cmd. For more information on S3, including local installation instructions, refer to DigitalOcean's [Setting Up s3cmd 2.x with DigitalOcean Spaces reference](#).

Rationale:

Creating a lifecycle configuration rule is important for the following reasons:

- **Data management:** Lifecycle rules automate the management process, ensuring that data is handled systematically according to predefined policies. This reduces the likelihood of human error and the administrative burden associated with manual data management.
- **Risk Mitigation:** Proper data lifecycle management helps in mitigating risks associated with data breaches. By ensuring that data is only stored as long as necessary, lifecycle rules reduce the volume of sensitive data at risk.
- **Compliance:** Many industries are governed by regulations that require data to be retained for certain periods and deleted thereafter. Lifecycle rules help ensure compliance with such regulations automatically, reducing the risk of costly legal or regulatory penalties.

Impact:

A significant risk associated with lifecycle configuration rules is unintended data loss. For example, if the expiration period is set too short, data might be deleted before its utility has expired. Another potential risk is not aligning lifecycle rules with compliance and security policies as that presents the risk of violating legal or regulatory requirements.

A lifecycle rule that deletes a large amount of objects can take hours or days to finish running. During this process, you are still billed for any objects that have not been deleted yet. To delete objects faster, use the [S3 DeleteObject or DeleteObjects commands](#).

Audit:

1. List your Spaces.

```
s3cmd ls
```

2. Get the lifecycle policy for your selected Space.

```
s3cmd getlifecycle s3://selected-space
```

3. If no lifecycle configurations exist, the following message will be displayed

```
ERROR: S3 error: 404 (NoSuchLifecycleConfiguration)
```

Remediation:

Lifecycle rules can be used to perform different actions on objects in a Spaces bucket over the course of their “life.” For example, a Spaces bucket may be configured so that objects in it expire and are automatically deleted after a certain length of time. Lifecycle rules based on tagging are not supported.

Before creating lifecycle rules, [set up s3cmd 2.x with DigitalOcean Spaces](#).

Follow these steps after setting up s3cmd:

Set an Expiration Rule

To automatically delete objects after a set number of days, run the following command, substituting **<your-space-name>** with the name of your Spaces bucket:

```
s3cmd expire --expiry-days=30 --expiry-prefix= s3://<your-space-name>
```

In this command, the lifecycle rule rule expires all objects in your specified Space 30 days after their creation.

Remove Incomplete Multipart Uploads

To automatically remove incomplete multipart uploads after a set number of days, run the following command, substituting **<your-space-name>** with the name of your Spaces bucket:

```
s3cmd expire --expiry-mpu-days=1 s3://your-space-name
```

This command prevents abandoned multipart uploads from consuming storage unnecessarily after 1 day.

For more details, see the [s3cmd documentation](#).

References:

1. <https://docs.digitalocean.com/products/spaces/reference/s3cmd/>

2. <https://docs.digitalocean.com/products/spaces/reference/s3-compatibility/>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

5.4 Ensure File Listing Permissions are Set (Manual)

Profile Applicability:

- Level 1

Description:

A Spaces bucket's file listing is a list of the bucket's contents in XML. It displays the names (called keys) of every file in the bucket as well as other file information, like the file sizes and last modified dates.

Owners of a bucket set the visibility permissions of this file listing, which can be:

- **Public:** Anyone on the internet can view the listing by visiting the base URL of the bucket, even if the contents of individual files are set to Private.
- **Private:** Only users who connect to the bucket using access keys can see the contents.

You can set the visibility of the file listing when [creating a bucket](#). On existing buckets, you can view and edit the permissions on the bucket's Settings tab. The bucket's Settings tab can be found by selecting the individual bucket from the [Spaces Access Keys](#) landing page.

Rationale:

Setting the file listing permission is important for several reasons, including:

- **Preventing Unauthorized Access:** Public file listings can give attackers insight into the structure and contents of your storage. If they can see files that should remain private, they might attempt to access them. Properly setting file listing permissions can help reduce this risk.
- **Resource Control:** Public file listings can lead to unnecessary or unintended traffic, as users or bots may try to access files they don't need. By restricting file listing access, you have more control over who can access your resources, helping to reduce unnecessary bandwidth usage and avoid overloading your systems with irrelevant requests.

Impact:

Setting the file listing to **Public** exposes individual files you may want to keep private. To keep files private, store them in a private bucket. Setting the file listing to **Private** requires careful access policy design and ongoing management.

Audit:

1. From the [control panel](#), select **Spaces Object Storage**.
2. Navigate to the bucket's detail page by clicking the name of the bucket.

3. Click the **Settings** tab.
4. Locate the listing permission in the **File Listing** row.

Remediation:

You can set the visibility of the list of contents when [creating a bucket](#). On existing buckets, you can view and edit it on the bucket's **Settings** tab, in the **File Listing** section.

The Spaces file listing looks similar to this:

```
<ListBucketResult xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
  <Name>permissions</Name>
  <Prefix/>
  <Marker/>
  <MaxKeys>1000</MaxKeys>
  <IsTruncated>>false</IsTruncated>
  <Contents>
    <Key>example-file.txt</Key>
    <LastModified>2017-09-17T19:20:21.360Z</LastModified>
    <ETag>"39365ac292b6471ef008d1099bf99963"</ETag>
    <Size>42</Size>
    <StorageClass>STANDARD</StorageClass>
    <Owner>
      <ID>2900818</ID>
      <DisplayName>2900818</DisplayName>
    </Owner>
  </Contents>
  <Contents>
    <Key>image.png</Key>
    <LastModified>2017-09-17T23:19:53.222Z</LastModified>
    <ETag>"00d3c043c2e54e99712d6e526932bb76"</ETag>
    <Size>95607</Size>
    <StorageClass>STANDARD</StorageClass>
    <Owner>
      <ID>2900818</ID>
      <DisplayName>2900818</DisplayName>
    </Owner>
  </Contents>
</ListBucketResult>
```




Default Value:

The permission to list the contents of a DigitalOcean Spaces bucket is **Private** by default.

References:

1. <https://docs.digitalocean.com/products/spaces/how-to/create/>
2. https://cloud.digitalocean.com/spaces/access_keys?i=0b04d4
3. <https://docs.digitalocean.com/products/spaces/how-to/set-file-listing-permissions/>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			

5.5 Ensure Spaces CDN is Enabled (Manual)

Profile Applicability:

- Level 2

Description:

Spaces provides a built-in content delivery network (CDN), which is a network of edge servers that deliver content to users. Each point of presence (PoP), the location of a group of edge servers, sends content to the users that are physically closest to it. CDNs help deliver static and dynamic online content faster and more reliably, and provides a layer of redundancy for websites.

Rationale:

Enabling the Spaces CDN is important for several reasons, including:

- **DDoS Protection:** CDNs help protect against distributed denial-of-service (DDoS) attacks by mitigating malicious traffic over a network.
- **Built-in Bot Management:** CDNs can block malicious bots to prevent scraping and spam attacks, among other threats.
- **Improved Performance and Speed:** The CDN caches your content in multiple locations, reducing the distance between your users and the server hosting your data. This results in faster load times for your content.
- **Reliability and Redundancy:** The CDN provides redundancy and fault tolerance by distributing your content across multiple servers. If one server or data center fails, traffic is automatically rerouted to another, ensuring your content remains accessible without downtime.

Impact:

We do not recommend or support using multiple CDNs from separate vendors with your Spaces buckets (such as the Spaces built-in CDN and another vendor's CDN), as it can cause performance issues and be complex to manage.

Audit:

1. From the control panel, select [Spaces Object Storage](#).
2. Navigate to the bucket's detail page by clicking the name of the bucket.
3. Click the **Settings** tab.
4. Locate the CDN's classification in the **CDN (Content Delivery Network)** section.
5. If **Disabled**, follow the steps in the **Description** to **Enable the CDN**.

Remediation:

Enable the CDN during Bucket Creation

The Spaces CDN can be enabled during bucket creation by identifying the CDN (Content Delivery Network) section on the [Spaces create page](#).

Click **Enable CDN**. An Edge Cache TTL drop-down menu will appear. This setting determines the amount of time that the content is cached. You can keep the default of 1 hour or choose another value. You can also [customize the CDN endpoint](#) with a secure subdomain you own.

Finish choosing the rest of the settings for the bucket, then click **Create a Space**. Once the bucket is created, you can modify the edge cache TTL setting and custom subdomain at any time on the bucket's Settings page.

Enable the CDN for an Existing Bucket

1. The Spaces CDN can be enabled for an existing bucket. From the [Control Panel](#), navigate to the bucket's detail page by selecting **Spaces Object Storage** and subsequently, selecting the name of the bucket.
2. Click the **Settings** tab. The text in the CDN (Content Delivery Network) section will tell you if the CDN is currently Enabled or Disabled for the bucket.
3. To enable the CDN, in the same CDN (Content Delivery Network) section, click **Edit**.
4. In the options that open, click **Enable CDN**. When you do, several options for the CDN will appear. You can [customize the CDN endpoint](#) with a secure subdomain you own using the Use a custom subdomain menu. The Edge Cache TTL determines the amount of time that the content is cached. You can keep the default of 1 hour or choose another value.
5. When you're done choosing options, click **Save**. Once the CDN is enabled, you can return to this page to modify the edge cache TTL setting and custom subdomain.

References:

1. <https://cloud.digitalocean.com/spaces/new>
2. <https://docs.digitalocean.com/products/spaces/how-to/customize-cdn-endpoint/>
3. <https://cloud.digitalocean.com/>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

5.6 Ensure CORS is Enabled (Manual)

Profile Applicability:

- Level 2

Description:

Client web applications loaded in one domain can interact with resources in a Spaces bucket with [Cross-Origin Resource Sharing \(CORS\)](#) configured.

Rationale:

Configuring CORS for a Spaces bucket is important for several reasons, including:

- **Improved Content Delivery:** If your web app needs to serve static assets from a Spaces bucket, CORS enables these assets to be used in your application even when they reside in different origins. It helps in delivering these assets efficiently across different domains without encountering browser restrictions.
- **Access Control:** With CORS, you can set specific policies on which domains are allowed to interact with your Spaces bucket, which HTTP methods are allowed, and which headers can be used. This provides control over who can access your data and under what conditions, helping you maintain security while enabling cross-origin resource sharing.

Impact:

Overly permissive CORS can expose your data to unauthorized applications.

Audit:

1. From the [control panel](#), select **Spaces Object Storage**.
2. Navigate to the bucket's detail page by clicking the name of the bucket.
3. Click the **Settings** tab.
4. Locate the applicable configurations within the **CORS Configurations section**.

Remediation:

1. From the [control panel](#), navigating to the designated bucket's **Settings** page.
2. In the CORS Configuration row, click **Add**.

This opens the **Advanced CORS Options** window.

Within the Advanced CORS Options window, the following can be completed:

- **Origin:** Specifies the complete domain of the client you want to access your bucket's resources. The domain should start with a protocol identifier, such as http, end with a hostname or hostname and port, and optionally include a wildcard character () *at the start of the hostname*. For example,

****https://.example.com****. All other settings are only applied to requests from this Origin.

- **Allowed Methods:** Determines which API methods can interact with your bucket. You can allow or prohibit the following methods:
 - **GET:** Downloads a resource.
 - **PUT:** Updates a resource's properties or information.
 - **DELETE:** Deletes a resource.
 - **POST:** Creates a new resource.
 - **HEAD:** Retrieves a resource's metadata, such as its file size.
- **Allowed Headers:** Determines which non-default headers are accepted in your bucket. To verify that an incoming HTTP request abides by your CORS settings, your bucket checks the request's list of headers. Each header describes a property of the request. For example, Content-Length and Content-Type are some of the default headers that CORS automatically accepts. However, if your client sends any non-default headers, you must first add them in your CORS configuration.
- **Access Control Max Age:** Determines how long a request's verification is cached, in seconds. While verification is cached, the bucket can accept more requests from the same origin without needing to be verified, which improves performance. The recommended value is 5 seconds. Lower values may be useful during development, and higher values may be useful if a single browser is issuing many requests at once. Some browsers may also limit this value to as high as 10 minutes.

CORS configurations unavailable via the control panel, such as **ExposeHeaders**, can be implemented by [uploading a configuration XML file](#) via s3cmd. Please visit [this tutorial](#) for more information about setting up s3cmd.

For example, the following XML file sets **ExposeHeaders** to **ETag**, alongside other configuration options:

```
<CORSConfiguration xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
  <CORSRule>
    <AllowedOrigin>*</AllowedOrigin>
    <AllowedMethod>POST</AllowedMethod>
    <AllowedMethod>PUT</AllowedMethod>
    <AllowedMethod>DELETE</AllowedMethod>
    <MaxAgeSeconds>3000</MaxAgeSeconds>
    <ExposeHeader>ETag</ExposeHeader>
    <AllowedHeader>*</AllowedHeader>
  </CORSRule>
</CORSConfiguration>
```

You can then upload an XML configuration file to your bucket with the following s3cmd command:

```
s3cmd setcors /path/to/config.xml s3://BUCKET_NAME
```

References:

1. <https://developer.mozilla.org/en-US/docs/Web/HTTP/Guides/CORS>

2. <https://cloud.digitalocean.com/>
3. <https://docs.digitalocean.com/products/spaces/reference/s3cmd/>
4. <https://docs.digitalocean.com/products/spaces/how-to/configure-cors/#xml>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

5.7 Ensure Unneeded Spaces Bucket are Destroyed (Manual)

Profile Applicability:

- Level 2

Description:

Destroying a Spaces bucket permanently and irrecoverably destroys the bucket and all of its objects. When you confirm the destruction of your last bucket, your Spaces subscription ends automatically and you are no longer charged.

Rationale:

Destroying a Spaces bucket is important for several reasons, including:

- **Data leak prevention:** Deleting buckets that are no longer needed ensures that old or sensitive data is not accidentally exposed or accessed by unauthorized parties.
- **Cost control:** Spaces buckets incur storage costs, so destroying unused buckets can help minimize expenses. Your Spaces subscription automatically ends when you destroy all your buckets.

Impact:

In the event buckets targeted for destruction no longer need to be destroyed, not cancelling bucket destruction before its destruction time leads to permanent data loss.

Audit:

1. From the [control panel](#), select **Spaces Object Storage**.
2. Locate the bucket which has been targeted for deletion.
3. Confirm the designated bucket is greyed out, which means the bucket is pending destruction and the Overview page and More menu are not viewable.

Remediation:

Destroying a Spaces bucket permanently and irrecoverably destroys the bucket and all of its objects. When you confirm the destruction of your last bucket, your Spaces subscription ends automatically and you are no longer charged.




1. To destroy a bucket, click its name on [the Spaces page](#) to go to its detail page, then click the **Settings** tab.
2. In the **Destroy this Space** section, click **Destroy** to open the **Destroy Space** configuration window. Enter the name of the bucket and click Destroy to confirm.

When you confirm the destruction, the bucket goes into a pending destruction stage. The bucket remains listed in the control panel with an estimated time of destruction, and it is greyed out so you can't view its overview page or open its **More** menu. The bucket's scheduled destruction time is 2 weeks or more, depending on the size of the bucket. While a bucket is pending destruction, you cannot use it, it no longer counts towards your billing charges, and you cannot reuse its name. To cancel the destruction and regain access to your bucket, click **Cancel Deletion** before the scheduled deletion time.

References:

1. <https://cloud.digitalocean.com/spaces>
2. <https://cloud.digitalocean.com/>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.5 <u>Securely Dispose of Data</u> Securely dispose of data as outlined in the enterprise's data management process. Ensure the disposal process and method are commensurate with the data sensitivity.			

6 Volumes

This section contains recommendations for configuring DigitalOcean Volumes for improved security.

6.1 Ensure Drive is Encrypted with LUKS on Top of Volume (Manual)

Profile Applicability:

- Level 2

Description:

DigitalOcean Volumes are scalable, SSD-based block storage devices. Volumes allow you to create and expand your infrastructure's storage capacity without needing to resize your Droplets.

Volumes are encrypted at rest, which means that the data on a Volume is not readable outside of its storage cluster. When you attach a Volume to a Droplet, the Droplet is presented with a decrypted block storage device and all data is transmitted over isolated networks.

For additional security, you can also create a file system in a LUKS (Linux Unified Key Setup) encrypted disk on your Volume. This means that the disk will need to be decrypted by the operating system on your Droplet in order to read any data.

Rationale:

Encrypting the file system of your Volume Block Storage is important for several reasons:

- **Data Protection:** Encryption ensures that data is protected from unauthorized access, both during storage and transit.
- **Security Compliance:** It helps meet regulatory and compliance requirements that mandate data encryption.
- **Mitigation of Data Breaches:** In the event of a security breach, encrypted data remains inaccessible without the encryption keys.
- **Confidentiality:** Sensitive information remains confidential, ensuring privacy and trust.

Impact:

This process is destructive to any data on the Volume. Be sure to either start with a new Volume or back up your data before reformatting an existing Volume.

Encryption and decryption processes can introduce latency, impacting read/write speeds and overall system performance.

Good practices for preventing data loss are:

- Always back up your data before encrypting or modifying any partition.
- If you're new to encryption, test on a non-critical partition or virtual disk first.
- Double-check commands before executing them to avoid accidental data loss.-

Audit:

Use the following script to check if the disk is encrypted:

```
cryptsetup status secure-volume
```

Expected output for an inactive device will look similar to this:

```
/dev/mapper/secure-volume is inactive
```

Expected output for an active device will look similar to this:

```
/dev/mapper/secure-volume is active and is in use.  
type: LUKS2  
cipher: aes-xts-plain64  
keysize: 512 bits  
key location: keyring  
device: /dev/sda  
sector size: 512  
offset: 32768 sectors  
size: 209682432 sectors  
mode: read/write
```

Remediation:

Install Cryptsetup

cryptsetup is a utility used to manage LUKS volumes in addition to other encrypted formats.

Debian/Ubuntu

```
sudo apt-get install cryptsetup  
sudo apt install cryptsetup
```

CentOS

```
sudo yum install cryptsetup
```

Fedora

```
sudo dnf install cryptsetup
```

Creating the Encrypted Disk

1. Use **cryptsetup** to initialize an encrypted disk on your Volume.

```
sudo cryptsetup -y -v luksFormat /dev/disk/by-id/scsi-0DO_Volume_<volume-  
lon1-01>
```

Make sure to replace **volume-lon1-01** with the name of your Volume. The **-y** flag will require you to enter your passphrase twice when you're prompted to create it. The **-v** flag adds additional human-readable output to verify the success of the command. The output will ask you to confirm overwriting the data on the Volume. Type **YES** in all caps, then press **ENTER** to continue.

```
WARNING!
=====
This will overwrite data on /dev/disk/by-id/scsi-0DO_Volume_volume-lon1-01
irrevocably.

Are you sure? (Type uppercase yes): YES
```

2. Next, the output will prompt you to create a passphrase for the encrypted disk. Enter a unique, strong passphrase and verify it by entering it a second time. This passphrase is not recoverable, so keep it recorded in a safe place.

```
. . .
Enter passphrase:
Verify passphrase:
Command successful.
```

If you need to, you can change this passphrase in the future with the **cryptsetup luksChangeKey** command. You can also add up to 8 additional passphrases per device with **cryptsetup luksAddKey**.

3. At this point, your disk is created and encrypted. Next, decrypt it and map it to a label for easier referencing. Here, we're labeling it **name-of-volume**, but you can label it with anything you like.

```
sudo cryptsetup luksOpen /dev/disk/by-id/scsi-0DO_Volume_volume-lon1-01 name-
of-volume
```

You'll be prompted for the passphrase. Once you enter it, the Volume will now be mapped to **/dev/mapper/name-of-volume**.

4. To make sure everything worked, verify the details of the encrypted disk.

```
cryptsetup status name-of-volume
```

You'll see output like this indicating the Volume label and type:

```
/dev/mapper/name-of-volume is active.
type:      LUKS1
cipher:    aes-xts-plain64
keysize:   256 bits
device:    /dev/sda
offset:    4096 sectors
size:      209711104 sectors
mode:      read/write
```

At this point, you have a passphrase-protected encrypted disk. The next step is to create a file system on that disk so the operating system can use it to store files.

Creating and Mounting the File System

1. Look at the current available disk space on the Droplet.

```
df -h
```

You'll see output similar to this, depending on your Droplet configuration:

Filesystem	Size	Used	Avail	Use%	Mounted on
udev	2.0G	0	2.0G	0%	/dev
tmpfs	396M	5.6M	390M	2%	/run
/dev/vda1	78G	877M	77G	2%	/
tmpfs	2.0G	0	2.0G	0%	/dev/shm
tmpfs	5.0M	0	5.0M	0%	/run/lock
tmpfs	2.0G	0	2.0G	0%	/sys/fs/cgroup
/dev/vda15	105M	3.4M	101M	4%	/boot/efi
tmpfs	396M	0	396M	0%	/run/user/1000

At this point, `/dev/mapper/name-of-volume` doesn't show up on this list because the Volume isn't yet accessible to the Droplet. To make it accessible, you need to create and mount the file system.

2. Use the `mkfs.xfs` utility (make file system) to create an [XFS](#) file system on the volume.

```
sudo mkfs.xfs /dev/mapper/name-of-volume
```

Once the file system is created, you can [mount](#) it, which means making it available to the operating system on your Droplet.

3. Create a *mount point*, which is where the file system will be attached. A good recommendation for a mount point is an empty directory in the `/mnt` directory, so we'll use `/mnt/secure`.

```
sudo mkdir /mnt/secure
```

4. Mount the file system.

```
sudo mount /dev/mapper/name-of-volume /mnt/secure
```

5. To make sure it worked, check the available disk space on your Droplet again:

```
df -h
```

6. You'll now see `/dev/mapper/name-of-volume` listed.


```

Output
Filesystem                Size      Used Avail Use% Mounted on
udev                     2.0G         0   2.0G   0% /dev
tmpfs                    396M     5.6M   390M   2% /run
/dev/vda1                 78G     877M    77G   2% /
tmpfs                     2.0G         0   2.0G   0% /dev/shm
tmpfs                     5.0M         0   5.0M   0% /run/lock
tmpfs                     2.0G         0   2.0G   0% /sys/fs/cgroup
/dev/vda15                105M     3.4M    101M   4% /boot/efi
tmpfs                     396M         0   396M   0% /run/user/1000
/dev/mapper/name-of-volume 100G      33M   100G   1% /mnt/secure

```

This means your encrypted file system is attached and available for use.

When you no longer need to access the data on the Volume, you can unmount the file system and lock the encrypted disk.

You can verify with `df -h` that the file system is no longer available. In order to make the data on the Volume accessible again, you would run through the steps to open the disk (`cryptsetup luksOpen ...`), create a mount point, and mount the file system.

To avoid going through this manual process every time you want use the Volume, you can instead configure the file system to mount automatically when your Droplet boots.

Automatically Mounting the File System on Boot

The encrypted disk can have up to 8 passphrases. In this final step, we'll create a key and add it as a passphrase, then use that key to configure the Volume to be decrypted and mounted as the Droplet is booting.

1. Create a key file at `/root/.secure_key`. This command will make a 4 KB file with random contents:

```
sudo dd if=/dev/urandom of=/root/.secure-key bs=1024 count=4
```

2. Adjust the permissions of this key file so it's only readable by the root user.

```
sudo chmod 0400 /root/.secure-key
```

3. Add the key as a passphrase for the encrypted disk.

```
cryptsetup luksAddKey /dev/disk/by-id/scsi-0DO_Volume_volume-lon1-01
/root/.secure-key
```

You'll be prompted for a passphrase. You can enter the one you set when you first created the encrypted disk.

4. `/etc/crypttab` is a configuration file that defines encrypted disks to set up when the system starts. Open this file with `nano` or your favorite text editor.

```
sudo nano /etc/crypttab
```

5. Add the following line to the bottom of the file to map the Volume at boot:

```
name-of-volume /dev/disk/by-id/scsi-0DO_Volume_volume-lon1-01 /root/.secure-key luks
```

The format of the lines in `/etc/crypttab` is `device_name device_path key_path options`. Here, the device name is `name-of-volume` (or the name you chose instead), the path is `/dev/disk/by-id/...`, the key file is what we just created at `/root/.secure_key`, and the options specify `luks` encryption.

6. Save and close the file.
7. `/etc/fstab` is a configuration file to automate mounting. Open this file for editing.

```
sudo nano /etc/fstab
```

8. Add the following line to the bottom of the file to automatically mount the disk at boot:

```
/dev/mapper/name-of-volume /mnt/secure xfs defaults,nofail 0 0
```

The first three arguments of the lines in `/etc/fstab` are always `device_path mount_point file_system_type`. Here, we have the same device path and mount point as in Step 2, and we specify the XFS file system. You can read about the other fields in `fstab`'s man page (`man fstab`).

9. Save and close the file. Your encrypted file system is now set to automatically mount when your Droplet boots. You can test this by rebooting your Droplet, but be cautious with any running services.




Default Value:

By default, DigitalOcean Volumes are encrypted when they are not attached to a Droplet.

References:

1. <https://en.wikipedia.org/wiki/XFS>
2. <https://www.digitalocean.com/community/tutorials/how-to-partition-and-format-digitalocean-block-storage-volumes-in-linux#mounting-the-filesystems>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.11 <u>Encrypt Sensitive Data at Rest</u> Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.			
v7	14.8 <u>Encrypt Sensitive Information at Rest</u> Encrypt all sensitive information at rest using a tool that requires a secondary authentication mechanism not integrated into the operating system, in order to access the information.			

Appendix: Summary Table

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1	Introduction		
1.1	CIS DigitalOcean Foundations Benchmarks		
1.2	CIS DigitalOcean Services Benchmarks		
2	Droplet		
2.1	Ensure Backups are Enabled (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.2	Ensure a Firewall is Created (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3	Ensure the Droplet is Connected to a Firewall (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.4	Ensure Operating System on Droplet is Upgraded (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.5	Ensure Operating System is Updated (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.6	Ensure Auditd is Enabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.7	Ensure SSH Keys are Used to Authenticate (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.8	Ensure Unused SSH Keys are Deleted (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3	Kubernetes		
3.1	Ensure Log Forwarding is Enabled (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
3.2	Ensure an Upgrade Window is Defined (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.3	Ensure High Availability Control Plane is Enabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4	Logging and Monitoring		
4.1	Ensure Security History is Monitored (Manual)	<input type="checkbox"/>	<input type="checkbox"/>

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
4.2	Ensure Resource Monitoring is Enabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5	Spaces		
5.1	Ensure Access Control to Spaces are Set (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
5.2	Ensure Access and Secret Keys are Created (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
5.3	Ensure Spaces Bucket Lifecycle Policy is Set (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.4	Ensure File Listing Permissions are Set (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
5.5	Ensure Spaces CDN is Enabled (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
5.6	Ensure CORS is Enabled (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
5.7	Ensure Unneeded Spaces Bucket are Destroyed (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
6	Volumes		
6.1	Ensure Drive is Encrypted with LUKS on Top of Volume (Manual)	<input type="checkbox"/>	<input type="checkbox"/>

Appendix: CIS Controls v7 IG 1 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
2.1	Ensure Backups are Enabled	<input type="checkbox"/>	<input type="checkbox"/>

Appendix: CIS Controls v7 IG 2 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
2.1	Ensure Backups are Enabled	<input type="checkbox"/>	<input type="checkbox"/>

Appendix: CIS Controls v7 IG 3 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
2.1	Ensure Backups are Enabled	<input type="checkbox"/>	<input type="checkbox"/>
6.1	Ensure Drive is Encrypted with LUKS on Top of Volume	<input type="checkbox"/>	<input type="checkbox"/>

Appendix: CIS Controls v7 Unmapped Recommendations

Recommendation		Set Correctly	
		Yes	No
2.2	Ensure a Firewall is Created	<input type="checkbox"/>	<input type="checkbox"/>
2.3	Ensure the Droplet is Connected to a Firewall	<input type="checkbox"/>	<input type="checkbox"/>
2.4	Ensure Operating System on Droplet is Upgraded	<input type="checkbox"/>	<input type="checkbox"/>
2.5	Ensure Operating System is Updated	<input type="checkbox"/>	<input type="checkbox"/>
2.6	Ensure Auditd is Enabled	<input type="checkbox"/>	<input type="checkbox"/>
2.7	Ensure SSH Keys are Used to Authenticate	<input type="checkbox"/>	<input type="checkbox"/>
2.8	Ensure Unused SSH Keys are Deleted	<input type="checkbox"/>	<input type="checkbox"/>
3.1	Ensure Log Forwarding is Enabled	<input type="checkbox"/>	<input type="checkbox"/>
3.2	Ensure an Upgrade Window is Defined	<input type="checkbox"/>	<input type="checkbox"/>
3.3	Ensure High Availability Control Plane is Enabled	<input type="checkbox"/>	<input type="checkbox"/>
4.1	Ensure Security History is Monitored	<input type="checkbox"/>	<input type="checkbox"/>
4.2	Ensure Resource Monitoring is Enabled	<input type="checkbox"/>	<input type="checkbox"/>
5.1	Ensure Access Control to Spaces are Set	<input type="checkbox"/>	<input type="checkbox"/>
5.2	Ensure Access and Secret Keys are Created	<input type="checkbox"/>	<input type="checkbox"/>
5.3	Ensure Spaces Bucket Lifecycle Policy is Set	<input type="checkbox"/>	<input type="checkbox"/>
5.4	Ensure File Listing Permissions are Set	<input type="checkbox"/>	<input type="checkbox"/>
5.5	Ensure Spaces CDN is Enabled	<input type="checkbox"/>	<input type="checkbox"/>
5.6	Ensure CORS is Enabled	<input type="checkbox"/>	<input type="checkbox"/>
5.7	Ensure Unneeded Spaces Bucket are Destroyed	<input type="checkbox"/>	<input type="checkbox"/>

Appendix: CIS Controls v8 IG 1 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
2.1	Ensure Backups are Enabled	<input type="checkbox"/>	<input type="checkbox"/>
2.4	Ensure Operating System on Droplet is Upgraded	<input type="checkbox"/>	<input type="checkbox"/>
2.5	Ensure Operating System is Updated	<input type="checkbox"/>	<input type="checkbox"/>
2.7	Ensure SSH Keys are Used to Authenticate	<input type="checkbox"/>	<input type="checkbox"/>
2.8	Ensure Unused SSH Keys are Deleted	<input type="checkbox"/>	<input type="checkbox"/>
3.2	Ensure an Upgrade Window is Defined	<input type="checkbox"/>	<input type="checkbox"/>
5.1	Ensure Access Control to Spaces are Set	<input type="checkbox"/>	<input type="checkbox"/>
5.2	Ensure Access and Secret Keys are Created	<input type="checkbox"/>	<input type="checkbox"/>
5.4	Ensure File Listing Permissions are Set	<input type="checkbox"/>	<input type="checkbox"/>
5.7	Ensure Unneeded Spaces Bucket are Destroyed	<input type="checkbox"/>	<input type="checkbox"/>

Appendix: CIS Controls v8 IG 2 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
2.1	Ensure Backups are Enabled	<input type="checkbox"/>	<input type="checkbox"/>
2.2	Ensure a Firewall is Created	<input type="checkbox"/>	<input type="checkbox"/>
2.3	Ensure the Droplet is Connected to a Firewall	<input type="checkbox"/>	<input type="checkbox"/>
2.4	Ensure Operating System on Droplet is Upgraded	<input type="checkbox"/>	<input type="checkbox"/>
2.5	Ensure Operating System is Updated	<input type="checkbox"/>	<input type="checkbox"/>
2.7	Ensure SSH Keys are Used to Authenticate	<input type="checkbox"/>	<input type="checkbox"/>
2.8	Ensure Unused SSH Keys are Deleted	<input type="checkbox"/>	<input type="checkbox"/>
3.1	Ensure Log Forwarding is Enabled	<input type="checkbox"/>	<input type="checkbox"/>
3.2	Ensure an Upgrade Window is Defined	<input type="checkbox"/>	<input type="checkbox"/>
4.1	Ensure Security History is Monitored	<input type="checkbox"/>	<input type="checkbox"/>
4.2	Ensure Resource Monitoring is Enabled	<input type="checkbox"/>	<input type="checkbox"/>
5.1	Ensure Access Control to Spaces are Set	<input type="checkbox"/>	<input type="checkbox"/>
5.2	Ensure Access and Secret Keys are Created	<input type="checkbox"/>	<input type="checkbox"/>
5.4	Ensure File Listing Permissions are Set	<input type="checkbox"/>	<input type="checkbox"/>
5.7	Ensure Unneeded Spaces Bucket are Destroyed	<input type="checkbox"/>	<input type="checkbox"/>
6.1	Ensure Drive is Encrypted with LUKS on Top of Volume	<input type="checkbox"/>	<input type="checkbox"/>

Appendix: CIS Controls v8 IG 3 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
2.1	Ensure Backups are Enabled	<input type="checkbox"/>	<input type="checkbox"/>
2.2	Ensure a Firewall is Created	<input type="checkbox"/>	<input type="checkbox"/>
2.3	Ensure the Droplet is Connected to a Firewall	<input type="checkbox"/>	<input type="checkbox"/>
2.4	Ensure Operating System on Droplet is Upgraded	<input type="checkbox"/>	<input type="checkbox"/>
2.5	Ensure Operating System is Updated	<input type="checkbox"/>	<input type="checkbox"/>
2.7	Ensure SSH Keys are Used to Authenticate	<input type="checkbox"/>	<input type="checkbox"/>
2.8	Ensure Unused SSH Keys are Deleted	<input type="checkbox"/>	<input type="checkbox"/>
3.1	Ensure Log Forwarding is Enabled	<input type="checkbox"/>	<input type="checkbox"/>
3.2	Ensure an Upgrade Window is Defined	<input type="checkbox"/>	<input type="checkbox"/>
4.1	Ensure Security History is Monitored	<input type="checkbox"/>	<input type="checkbox"/>
4.2	Ensure Resource Monitoring is Enabled	<input type="checkbox"/>	<input type="checkbox"/>
5.1	Ensure Access Control to Spaces are Set	<input type="checkbox"/>	<input type="checkbox"/>
5.2	Ensure Access and Secret Keys are Created	<input type="checkbox"/>	<input type="checkbox"/>
5.4	Ensure File Listing Permissions are Set	<input type="checkbox"/>	<input type="checkbox"/>
5.7	Ensure Unneeded Spaces Bucket are Destroyed	<input type="checkbox"/>	<input type="checkbox"/>
6.1	Ensure Drive is Encrypted with LUKS on Top of Volume	<input type="checkbox"/>	<input type="checkbox"/>

Appendix: CIS Controls v8 Unmapped Recommendations

Recommendation		Set Correctly	
		Yes	No
2.6	Ensure Auditd is Enabled	<input type="checkbox"/>	<input type="checkbox"/>

Appendix: Change History

Date	Version	Changes for this version
Jul 29, 2025	1.0.0	Document Created