Secure eMail/Web Services

How to build a secure eMail server for professional use

Basic BlueOnyx startup instructions for building a DNS, eMail, and Web Server

In this guide, we will walk you through the essential steps to setup BlueOnyx, a comprehensive web hosting platform. BlueOnyx has been chosen for this guide based on extensive experience with its predecessors, BlueQuartz and the Cobalt Networks RaQ 550, which have proven to be reliable and efficient over the past 25 years. —Zeffie

OneAvenue LLC - OneAvenue.com

“There is no such thing as the cloud. It’s just somebody else’s computer”

DISCLAIMER - NOTICE

This document is intended to provide an introduction to setting up DNS and email servers. By using this document, you acknowledge and agree to the following terms:

1. No Relationship or Liability: The use of this document does not create any form of relationship or liability between the author and the user. This document is provided solely for educational purposes, and its use does not establish any professional relationship, nor does it imply any responsibility or liability on the part of the author.

2. Basics of Email Server Setup: This document outlines the basics of setting up an email server. It provides foundational information and guidance to help users get started with the process.

3. Additional Information: For more comprehensive information on making choices related to email services, readers should refer to the document "Internet Security for Attorneys" or qualified personal. These resources include additional decision-making information that may be crucial for ensuring the security and effectiveness of your email services.

4. Use at Your Own Risk: The information provided in this document is used at your own risk. The author makes no guarantees regarding the accuracy, completeness, or suitability of the information for any particular purpose.

5. No Warranty or Liability:
This document is provided "as is," without any warranty of any kind, either express or implied. The author and publisher have made every effort to ensure the accuracy of the information contained within this document. However, no warranty or fitness is implied. The author disclaims any and all liability for any damages or losses that may arise from the use of this document.

6. User Responsibility: Users of this document take full responsibility for the implementation and use of the information provided. It is the user's duty to

ensure that they follow best practices and seek additional guidance or professional assistance as necessary. Users are solely responsible for the application of the information contained herein.

7. Scope and Limitations: This document is not intended to cover every security topic related to DNS and email servers. It is designed to help users get up and running and is not a replacement for qualified personnel.

8. Trademarks: All brand names and product names used in this document are trade names, service marks, trademarks, or registered trademarks of their respective owners. The use of any trademark in this document does not vest in the author or publisher any trademark ownership rights in such trademarks, nor does the use of such trademarks imply any affiliation with or endorsement of this document by such owners.

9. Fair Use Declaration: This document includes references to various trademarks and proprietary products for educational purposes, under the principles of fair use, specifically for teaching, scholarship, and research purposes. The mention of these trademarks does not constitute an infringement of the respective owners' rights, particularly when used for critical, educational, or analytical purposes, and it should not be construed as such.

Any views or opinions are not intended to malign any religion, ethnic group, club, organization, company, or individual. The content of this document is for educational and informational purposes only and is intended for professionals.

This document is not affiliated with, sponsored by, or endorsed by any of the companies mentioned within it. All efforts have been made to ensure that entities are accurately represented, and any error or omission is unintentional and coincidental.

By proceeding with the use of this document, you agree to these terms and acknowledge that the author is not liable for any actions taken based on the information provided.

License Agreement

1. Grant of License
One Avenue LLC grants the buyer a non-exclusive, non-transferable license to use the “Do the Hillary" (the "Book") strictly for personal, non-commercial purposes. This license does not imply any right to distribute, sell, lease, or otherwise make the Book available to others in any form.

2. Ownership and Copyright
The Book is the property of One Avenue LLC and is protected by copyright laws and international copyright treaties, as well as other intellectual property laws and treaties. The purchase of this Book does not transfer any title to the intellectual property contained within it.

3. Restrictions on Use
This Book cannot be redistributed, resold, leased, licensed, sublicensed, or offered for use to another user. The contents of this Book may not be shared in any form of digital, print, or through any media without express written permission from One Avenue LLC. Unauthorized copying, duplication, or distribution of this Book is expressly forbidden.

4. Modification and Adaptation
Modifying, translating, adapting, or otherwise creating derivative works from the Book is prohibited without the prior written consent of One Avenue LLC.

5. Protection and Security
You agree to take all reasonable steps to protect the Book from unauthorized access, copying, or use. The Book is provided with a unique identifier that should not be removed, obscured, or altered in any manner.

6. Limitation of Liability
In no event will One Avenue LLC be liable for any special, incidental, indirect, or consequential damages whatsoever arising out of the use of or inability to use the Book, even if advised of the possibility of such damages.

7. Termination
This License is effective until terminated. The License will terminate immediately and without notice from One Avenue LLC if you fail to comply with any provision of this Agreement. Upon termination, you must destroy all copies of the Book in your possession.

8. General
This License constitutes the entire agreement between you and One Avenue LLC concerning the Book and supersedes any prior agreements or understandings, written or oral. This License may only be modified by a writing signed by an authorized officer of One Avenue LLC.

About: Author information

The author began their journey in technology in the early 1980s, starting with a Commodore computer and exploring the early online communities through platforms like CompuServe, Wildcat BBS, AOL, Genie, and Prodigy. They navigated a world where BBS numbers were essential for obtaining drivers from manufacturers and participating in public bulletin board systems where communities gathered to share information and resources.

In the early 1990s, the author took on a pivotal role in setting up and managing Microsoft "MS Mail" server services for a company of 200 people. The author provided critical data transfer services using modems and built robust networks using 10Base and 1-BaseT wiring. For over a decade, the author supported and maintained these systems, ensuring seamless communication and data flow within the organization. The author learned to have great respect for lighting.

By 1996, the author expanded their expertise to include internet hosting services, offering website, DNS, and mail services. This venture has continued to this day, showcasing a long-standing commitment to providing reliable and efficient internet eMail services. Today the company is called One Avenue llc.

The author's technical preferences reflect a broad and adaptable skill set. The author favors Linux for production systems due to its stability and performance, uses Windows for compatibility with various software and hardware, and appreciates Apple products for their ease of use, integration features, and potential security benefits. The author is well known as Zeffie from Zeffie.com

Education and Expertise

- RETS Electronics (1981 - 1982)
    - Certificate in Electronics, Interfacing, Programming, AI development
    - Grade: 3.9
    - Activities and Societies: Machine Code Club

At RETS Electronics, now known as NIT, the author gained a foundational understanding of computer operations, programming, and the integration of computers with external devices. The curriculum focused on industrial automation applications and emphasized troubleshooting, preparing students for careers in electronics repair and the development of AI systems.

Authors legal responsibilities as a Web Hosting company

Introduction:

In the realm of web hosting and information technology, the interplay between technical expertise and legal awareness is often under appreciated. As an IT professional deeply entrenched in this field, I have become increasingly cognizant of the crucial role that legal knowledge plays in our daily operations.

Navigating a Legal Minefield:

The digital landscape is fraught with legal complexities. In web hosting, every decision made and every service provided potentially treads on a minefield of legal considerations – from data privacy laws to intellectual property rights. My role necessitates a deep understanding of these legal frameworks to not only ensure compliance but also to safeguard our business and our clients from inadvertent legal transgressions.

The Burden of Compliance:

As a professional responsible for managing web hosting services, I am tasked with ensuring that our operations are not just technically sound, but also legally compliant. This involves a continuous process of monitoring regulatory changes, maintaining meticulous records, and managing risks. The job transcends the technical realm, venturing into legal territories that require a firm grasp of various compliance issues.

Legal Knowledge as a Shield:

In an era where data breaches and cyber-attacks are rampant, my legal awareness serves as a shield. It guides me in implementing robust data protection measures, respecting intellectual property rights, and adhering to contractual obligations. This knowledge is not merely about avoiding legal pitfalls, but about fostering trust and integrity in the services we provide.

The Intersection of Tech and Law:

In my journey as an IT expert, I have learned that technology does not exist in a vacuum. It is intertwined with legal, ethical, and societal dimensions. My opinions on the multitude of legal requirements in web hosting are shaped by this understanding. It's a testament to the evolving role of IT professionals in a world where tech decisions have far-reaching legal implications.

Legal Responsibilities of a Web Hosting Operator:

These responsibilities are integral to the role of a web hosting operator, ensuring that the service operates within the legal framework and maintains a high standard of compliance.

1. **Regulatory Compliance Monitoring:** Web hosting operators are required to continuously monitor and adhere to various laws and regulations. This involves staying updated on changes in data protection laws (like GDPR in Europe), copyright laws, and internet governance policies.

2. **Data Privacy and Protection:** Operators must ensure that their hosting services comply with data privacy laws. This involves managing how customer data is collected, stored, processed, and shared, in accordance with legal standards.

3. **Content Regulation Compliance:** They are responsible for understanding and enforcing content regulations. This includes monitoring hosted content to ensure it doesn't violate laws related to hate speech, intellectual property rights, and other relevant legal standards.

4. **Contractual Obligations and SLAs:** Maintaining adherence to the terms of service agreements and service level agreements (SLAs) with clients is crucial. This involves ensuring that all contractual obligations regarding uptime, data security, and customer support are met.

5. **Licensing and Intellectual Property Rights:** Web hosting operators must manage and adhere to the licensing requirements for any software or technology used in their services. They also need to respect and enforce intellectual property rights for the content hosted on their servers.

6. **Record Keeping and Documentation:** Maintaining detailed records of all compliance activities, user agreements, internal policies, and audits is a key legal responsibility. Proper documentation supports compliance and is essential for legal scrutiny and audits.

7. **Legal Correspondence and Reporting:** Operators are often required to respond to legal requests, including court orders or law enforcement requests related to hosted content or user activities. They must also prepare and submit compliance reports to regulatory bodies as required.

8. **Risk Management:** Identifying and mitigating risks related to legal non-compliance is a continuous responsibility. This includes conducting regular risk assessments and developing strategies to address identified risks.

9. **Customer Communication and Transparency:** Providing clear, transparent communication to customers about any legal and

compliance-related issues that may affect their service is essential. This also includes informing customers about their rights and obligations under both domestic and international law without giving legal advice.

10. **Dispute Resolution and Litigation Management:** Handling legal disputes, customer complaints, and potential litigation related to compliance issues forms part of their responsibilities. This includes working with legal counsel to address and resolve such issues.

11. **Policy Development and Training:** Developing internal policies to ensure compliance and training employees on these policies is crucial. This helps in creating a compliance-focused organizational culture.

12. **Vendor Compliance Management:** Ensuring that any third-party vendors or partners comply with relevant legal and regulatory requirements, especially concerning data handling and security.

The integration of legal knowledge into my IT skillset is not an added burden, but a necessary evolution of my role in the digital age. It empowers me to make informed decisions, protect our interests, and provide a service that is not only efficient but also compliant and ethical. As the digital landscape continues to evolve, so too will the legal challenges, and my commitment to staying informed and compliant remains steadfast.

In this guide, we will walk you through the essential steps to prepare for installing BlueOnyx, a comprehensive web hosting platform. BlueOnyx has been chosen for this guide based on extensive experience with its predecessors, BlueQuartz and the Cobalt Networks RaQ 550, which have proven to be reliable and efficient over the past 25 years.

Authors Current Focus:

As of 2024, the author is concentrating on developing new AI information systems tailored for special needs applications. Leveraging advanced coding techniques, they aim to create customized solutions that improve accessibility and support for individuals with unique requirements.

This work represents a commitment to innovation and inclusivity, ensuring that technology serves and empowers all users.

This comprehensive background and dedication to technology demonstrate the author's extensive expertise and ongoing passion for leveraging technology to solve real-world problems and enhance user experiences.

eMail server history

Introduction

Setting up your own DNS and email server has always been the prudent thing to do for those concerned with data security and privacy. Historically, email services were primarily managed in-house, with systems like Microsoft Mail in the 1990s serving inter-office communications. External services like AOL Mail, popularized with the phrase "You've got mail," were used mainly for personal email rather than business communications. The concept of relying on outside services for critical data, especially email, was then—and remains—a security risk.

In the early days, companies that maintained their own email systems could ensure data security by keeping everything on-premises. This meant having direct control over the hardware and network, ensuring that sensitive information remained within the company's physical and digital boundaries.

The rise of cloud services has shifted this paradigm, largely driven by marketing efforts. Cloud service providers essentially offer remote servers that they manage, often assuming legal rights over the data stored on these servers. However, this arrangement does not always align with the stringent security requirements that businesses may have. The true security of data depends on who owns and controls the hardware and network that stores and transmits the data. Adding location

Building a secure, in-house email systems has always has been, quite straightforward. The fundamental components of email servers and DNS have remained largely unchanged over the years. What has evolved is the quality and reliability of internet connections (IP quality), which has improved significantly.

The software described here has provided the ability for anyone to set up a secure email server for over 25 years. While there are numerous other "systems" available to process mail, this one has always been in production and stable. With years of experience behind it, you can count on BlueOnyx to provide you with reliable eMail, Web and DNS services.

By setting up your own DNS and email server, you may retain full control over your data, ensuring it is secure and private. This document outlines the basics of setting up a DNS and email server, providing you with the knowledge and tools needed to take control of your email communications and data security.

About eMail server data Security in 2024

Why use a Private Email Server?

In today's digital age, securing your email communications is crucial, especially for professionals handling sensitive information. A private email server is essential not just for data protection but also for maintaining compliance and professional reputation.

In the current landscape of digital communications, professionals handling sensitive information face significant privacy and security risks. Many rely on third-party email service providers, which often leads to challenges such as:

- **Limited Privacy:** When emails are stored on third-party servers, the service provider has the legal right under federal law to access and use that data. This can lead to unintended disclosures, which are particularly sensitive in contexts like attorney-client communications.
- **Compliance Risks:** Regulatory requirements demand stringent data protection practices, especially for legal, healthcare, and financial sectors. Service providers may not always align with these specialized compliance needs.
- **Ownership Uncertainties:** Often, email service companies, especially those incorporated in jurisdictions with opaque ownership laws such as Delaware, can have unclear control over the data stored on their networks. This complexity can jeopardize the confidentiality and integrity of critical communications.
- **Operational Inefficiencies:** Generic email solutions may not offer the customization necessary to optimize workflows and communication within specialized fields.

These challenges underscore the need for a controlled, secure environment for email communications, where professionals can maintain autonomy over their data and ensure compliance with all applicable laws and ethical standards.

"The Secure Style" Mail Server
Inspired by high-profile scenarios, a secure email server ensures that your communications are hosted in a secure, private environment, giving you full control over your data.

Benefits of a Home or Office eMail Server

In today's digital age, securing your email communications is crucial, especially for professionals handling sensitive information. A home or office mail server provides a secure and private environment, giving you full control over your data. Here are the key benefits of setting up a local mail server:

Complete Control

Full Data Sovereignty: Hosting your email server locally allows you to control the environment and access to your data. You determine who can access your emails, how they are stored, and who has permissions to manage them. This ensures that your communications remain private and secure, free from third-party oversight and potential misuse.

Enhanced Security

Advanced Security Protocols: By managing your own mail server, you can implement advanced security measures to protect against unauthorized access and data breaches. Local email servers reduce the risk associated with third-party providers, ensuring that sensitive information remains within your control.

Compliance and Confidentiality

Meeting Legal Standards: Managing your own data security helps you meet legal standards and ethical obligations more effectively. This is particularly crucial for professionals who handle sensitive information and must adhere to strict confidentiality requirements. A local mail server allows you to implement and verify compliance measures directly.

Customization and Scalability

Tailored Solutions: A local email server can be customized to fit your specific needs, regardless of the size of your operations. Whether you are an individual professional or part of a larger team, you can scale your server setup to meet growing demands and integrate additional features as needed.

Conclusion

Setting up a home or office mail server offers numerous advantages, this approach provides a robust solution for professionals seeking to protect sensitive information and maintain autonomy over their data.

One Avenues additional services

Our comprehensive service is designed to assist you with the remote installation of a dedicated email server, including DNS configuration and ensuring your server operates on a reputable IP for optimal mail server performance. This package covers the complete installation of the operating system, tailored to meet the specific requirements of being a robust email server.

You'll benefit from unlimited hours of direct phone support and unlimited ticket support for 1 month, allowing you to resolve any issues quickly and efficiently. For ongoing needs, we offer optional monthly support plans which include continuous monitoring and maintenance to ensure your server remains secure, reliable, and up-to-date. This service is ideal for professionals who need a dependable email communication setup without the technical hassle.

Enhance Your Setup with Optional Products

Before you finalize your private email server configuration, consider integrating our optional enhancements to ensure the highest level of performance and reliability.

Secondary DNS Servers Expand your network infrastructure with three secondary DNS servers located strategically around the globe. This addition not only boosts your fault tolerance but also reduces latency, ensuring that your domain remains accessible and responsive at all times, no matter where your clients are located.

Email Relays Supplement your email setup with secondary mail servers. These servers act as powerful relays, enhancing email delivery speeds and adding an extra layer of redundancy. This is crucial for maintaining uninterrupted email communication, especially during high traffic periods or server maintenance windows.

These optional upgrades are particularly vital for professionals in the legal and medical field, where consistent access and secure communications are paramount. Enhancing your system with these robust solutions safeguards your operations against unexpected disruptions and keeps your client and patient communications smooth and professional.

These strategically positioned relays offer continuous online presence and network redundancy, essential for legal, medical and professional sectors where reliability is non-negotiable. Guaranteeing that every message is securely

accepted, our robust MX setup ensures uninterrupted email continuity and high dependability across multiple names.

Complementing the MX relays, our trio of secondary nameservers, located across the globe, enhances your DNS redundancy and speed. This setup provides robust fault tolerance and decreased latency, ensuring your domain remains accessible and resilient against outages. Each server is equipped with full IPv6 connectivity, offering compatibility and improved routing efficiency.

Fortify your communications framework with our resilient, globally located MX technology and nameserver architecture, designed to keep your professional operations smooth and uninterrupted. This powerful combination supports your need for absolute reliability in communication and domain stability.

When using our installation service please keep in mind…

- eMail servers require a static IP number provided by your internet service provider.
- Dual server installations require an additional IP.
- Static IPs are included in most internet service providers business plans.
- Residential internet services usually include IPs that are blocked by default from acting as mail servers.
- Check with your provider and we suggest a few extra IP's for additional servers if desired.
- We support only Linux systems from recognized providers.
- Windows Server and Exchange Server 2019 installation support is not included in this service.
- Running your own mail server requires a working 64 bit computer/server at your choice of location and is not included in this offer.
- These servers will also allow you to establish a private email address to complement your existing email services, such as YourName@secure.your-domain-name.com.

In this guide, we will walk you through the essential steps to prepare for installing BlueOnyx, a comprehensive web hosting platform. BlueOnyx has been chosen for this guide based on extensive experience with its predecessors, BlueQuartz and the Cobalt Networks RaQ 550, which have proven to be reliable and efficient over the past 20 years.

One Avenue: Secure eMail Setup Assistance

For those who prefer to have everything set up by professionals, our “Just Do It” service is the perfect solution. This one-time service ensures your email and optional web server are configured and running smoothly.

- **Initial Configuration**: We handle all the basic initial configuration, getting your local email and optional web server up and running efficiently.
- **Professional Setup**: For an additional one-time fee, you receive a professionally configured server without the stress and complexity of doing it yourself.

Why Choose One Avenue?

Choosing One Avenue means investing in top-tier support services that ensure your email server is set up correctly and maintained to the highest standards. Our expertise in configuring and supporting email servers guarantees that your communications infrastructure is reliable and secure. By leveraging our services, you can focus on your core business activities while we take care of the technical details.

Get Started Today

Ready to enhance your email server setup with One Avenue? Visit our website to add our services to your cart and take the first step towards a more secure and efficient communication system. Whether you opt for the comprehensive “Do the Hillary” package or the convenient “Just Do It” setup, One Avenue is here to support your professional communication needs every step of the way.

For more information or to get started with our services, please visit our website at oneavenue.com. Our dedicated team is ready to assist you with all your email server needs. Whether you have questions about our “Do the Hillary” package, the “Just Do It” setup, or any of our additional services, we’re here to help. Reach out today to ensure your communication infrastructure is secure, reliable, and professionally managed.

Introduction to BlueOnyx

BlueOnyx is an open-source hosting platform that provides web, email, DNS, and file transfer services through an intuitive web-based interface. It is designed to be easily installed on commodity hardware or virtual private servers, making it accessible for users of all technical levels. For more information, you can visit the official BlueOnyx website at blueonyx.it.

BlueOnyx traces its roots back to the original Cobalt Networks RaQ server appliances. These pioneering devices were renowned for their simplicity and effectiveness in managing server tasks. After Cobalt Networks was acquired by Sun Microsystems, the Sausalito GUI of the Cobalt RaQ550 and Qube3 was released as open-source software. This foundational software has since undergone significant modifications and improvements to remain functional on modern Linux operating systems, extending far beyond the original vision of its creators.

BlueOnyx has become a robust and reliable platform, excelling in server management and hosting services. It offers a comprehensive suite of services:

- Web Hosting: BlueOnyx supports both Apache and Nginx web servers, managing websites efficiently through virtual hosts.
- Email Services: The platform includes powerful mail server capabilities, supporting Postfix and Sendmail, with features like OpenDKIM integration and detailed email statistics.
- DNS Management: BlueOnyx simplifies DNS record creation and management, supporting both IPv4 and IPv6, along with DNSSEC and SPF record generation.
- File Transfer Services: It supports secure file transfers via FTP and SFTP, with optional chrooted jails.
- Database Management: The platform automates MySQL/MariaDB database creation and management, featuring tools like phpMyAdmin.
- Security Features: BlueOnyx offers two-factor authentication, SSH key/certificate management, brute force login detection, and support for multiple PHP versions.
- Additional Services: It includes CALDAV/CardDAV for calendar and contact management, Docker integration, and a built-in ticket and bug reporting system.

With its strong heritage and continuous evolution, BlueOnyx remains a trusted and versatile solution for modern server management and hosting needs.

IP Addresses for DNS and Mail Servers

When setting up DNS and mail servers, a comprehensive understanding of IP addresses is essential. Not all IP addresses are created equal; they vary based on their previous usage, location, network responsibility, and their status on various blacklists, such as Realtime Blackhole Lists (RBLs). These factors may significantly impact the functionality and reliability of your DNS and email servers.

Public IP Addresses
To operate DNS and mail servers effectively, you need public IP addresses. Public IPs are accessible over the internet and are crucial for external communication. Private IP addresses, on the other hand, are used within internal networks and are not routable on the internet.

IPv4 and IPv6 Addresses
There are two types of IP addresses: IPv4 and IPv6. IPv4 addresses are 32-bit numeric addresses written in decimal as four numbers separated by periods (e.g., 192.0.2.1). Due to the exponential growth of internet-connected devices, the IPv4 address space is becoming exhausted. IPv6 addresses, which are 128-bit alphanumeric addresses separated by colons (e.g., 2001:0db8:85a3:0000:0000:8a2e:0370:7334), were introduced to address this limitation.

Importance of Both IPv4 and IPv6
Modern internet infrastructure requires the use of both IPv4 and IPv6 addresses to ensure comprehensive connectivity and to mitigate various types of cyber-attacks. Utilizing both protocols enhances the resilience and reachability of your servers.

Reverse DNS
Maintaining reverse DNS (rDNS) is crucial when running DNS or mail servers. rDNS translates an IP address back to a domain name, which is often used by email servers to verify the legitimacy of the sending server. Properly configured rDNS can improve email deliverability and prevent your emails from being marked as spam.

Network Blacklists
Network blacklists, such as SORBS (Spam and Open Relay Blocking System), maintain lists of IP addresses that are known to be sources of spam or other malicious activities. These blacklists are used by mail servers to block incoming

connections from known bad actors. Being listed on one of these blacklists can severely impact your ability to send and receive emails.

Email RBLs
Email RBLs (Realtime Blackhole Lists) are another type of blacklist specifically used to filter out spam emails. There are numerous RBLs, each with its criteria and methods for listing IP addresses. Past activity associated with an IP, such as sending spam, can lead to its inclusion on these lists, resulting in delivery problems for legitimate emails.

Residential Lines and Port 25
Residential internet lines typically have port 25 (the default port for sending email) blocked by ISPs to prevent spam. Additionally, residential IPs are often self-listed on RBLs to prevent their use for sending emails due to their history of being exploited for spam.

Dynamic vs. Static IPs
Dynamic IPs change periodically and are typically assigned to residential users. Static IPs, however, remain constant and are essential for DNS and mail servers. Static IPs allow for consistent connectivity and are necessary for maintaining accurate DNS records and ensuring reliable email delivery.

Business Services and Static IPs
Business internet services often include static IPs, making them a better choice for setting up DNS and mail servers. These services provide the stability and reliability needed for server operations.

Conclusion and Requirements
Before building DNS and mail servers, it is important to verify the following:

- Ensure you have public IP addresses.
- Utilize both IPv4 and IPv6 addresses.
- Maintain proper reverse DNS configurations.
- Check the status of your IPs on network blacklists and email RBLs.
- Use static IPs to avoid connectivity issues and ensure consistent service.
- Confirm that your business service includes static IPs with adjustable PTR records for reverse DNS.

By addressing these considerations, you can establish a robust and reliable DNS and email server infrastructure.

DNS Name Server Basics

Setting up a DNS (Domain Name System) server is a crucial step for ensuring the reliability and security of your internet presence. DNS servers translate human-readable domain names into IP addresses that computers use to identify each other on the network.

For anyone responsible for maintaining a domain name, understanding how to properly set up DNS servers is essential. This guide will walk you through the key considerations and steps involved in setting up DNS servers.

Static IP Addresses

One of the fundamental requirements for setting up DNS servers is the use of static IP addresses. Unlike dynamic IP addresses, which change periodically, static IP addresses remain constant, ensuring that your DNS servers are always reachable at the same address. This stability is vital for the consistent operation of your DNS infrastructure.

Number of DNS Servers

Depending on your domain name registrar, you may be required to set up multiple DNS servers. Typically, up to six DNS servers can be registered. These servers provide redundancy, ensuring that if one server fails, others can take over, maintaining the availability of your domain.

Naming Conventions

While any name can be used for your DNS servers, the standard convention is to name them sequentially, such as ns1, ns2, ns3, and so on. For example, if your domain is example.com, your DNS servers might be named ns1.example.com, ns2.example.com, and ns3.example.com.

Glue Records

The IP addresses of your DNS servers must be registered as glue records with your domain registrar. Glue records are necessary when the names of your DNS servers are subdomains of the domain they serve. For instance, if your DNS server is ns1.example.com, the glue record will ensure that the DNS server can be located without relying on another DNS query, which would otherwise create a circular dependency.

Example Build: NS1.example.com

In our build example, we will use one server and call it NS1.example.com. This server will be configured with a static IP address and registered as a glue record with the domain registrar.

Geographic and Network Separation

To enhance reliability and provide failover capabilities, your DNS servers should be geographically and network separated. This means placing your servers in different physical locations and on different networks. Geographic and network separation ensures that a failure in one location or network does not affect the overall availability of your DNS services.

Secondary DNS Servers as Mail Relays

Secondary DNS servers can also serve as mail relays. This dual functionality can help in managing email delivery, especially in scenarios where the primary mail server is unavailable. By configuring your secondary DNS servers to act as backup mail servers, you can ensure that emails are not lost and are delivered reliably.

Conclusion

Setting up DNS servers with static IP addresses, proper naming conventions, and glue records is essential for maintaining a robust DNS infrastructure. Using multiple DNS servers, geographically and network-separated, provides redundancy and failover capabilities, reducing the risk of failures. Additionally, configuring secondary DNS servers as mail relays can further enhance email reliability.

By following these guidelines, you can create a reliable and resilient DNS setup that promotes uninterrupted internet and email services. Proper DNS configuration is a foundational aspect of maintaining a secure and efficient online presence, ensuring that your domain remains accessible and functional at all times.

IP Configuration for DNS and Mail Servers

Configuring IP addresses for DNS and mail servers is a critical aspect of ensuring reliable and efficient network operations. This article provides detailed guidance on how to properly set up your IP configuration, specifically addressing the needs of DNS and mail servers.

Primary Name Server Configuration

When setting up your DNS and mail server, the primary name server should be named something like ns1.example.com. This server will be your primary name server (NS1), and it plays a crucial role in your network's infrastructure.

Importance of the Primary Name Server (NS1)

- **DKIM Record Management:** Having a clearly defined primary name server simplifies the maintenance of DKIM (DomainKeys Identified Mail) records. DKIM records are essential for email deliverability, as they help verify that emails are not altered in transit and confirm the sender's identity. By managing DKIM records on NS1, you ensure they are consistently updated and properly maintained.
- **Synchronization with Secondary Name Servers:** Secondary name servers are configured to stay in sync with the primary name server (NS1). This synchronization ensures that any changes made to DNS records on NS1 are automatically propagated to the secondary servers, maintaining consistency and reliability across your network.
- **Organizational Clarity:** Naming your primary server NS1 and setting up secondary name servers in a similar hierarchical structure helps with organization, particularly when setting up email relays. Clear naming conventions make it easier to manage and troubleshoot your network infrastructure.

Main IP Address Configuration

The primary name server should be configured with the main IP address of your server. This IP address is crucial for the proper operation of your DNS and mail

servers. It is essential to keep your DNS records accurate and up-to-date, as any discrepancies can lead to service disruptions.

Keeping your Records in Order

Maintaining accurate DNS records is critical. Here are key points to consider:

- **Regular Updates:** Ensure that all changes to your DNS records are promptly updated on both primary and secondary name servers.
- **Consistency:** Verify that your DKIM records, MX (Mail Exchange) records, and other critical DNS entries are consistent and correct.
- **Monitoring:** Regularly monitor your DNS records to detect and rectify any discrepancies or errors.

Secondary Name Servers

In addition to your primary name server, you need at least one secondary name server located elsewhere to provide redundancy and failover capabilities. Secondary name servers can be configured with static IP addresses to ensure they are always reachable.

One Avenue Services

For those seeking reliable secondary name server options, One Avenue offers static name server services. By utilizing One Avenue's static nameservers, you can enhance the reliability and redundancy of your DNS and mail server infrastructure.

Conclusion

Getting the IP configuration for your DNS and mail servers correct is of utmost importance. By naming your primary name server ns1.example.com, managing DKIM records effectively, ensuring synchronization between primary and secondary servers, and keeping your DNS records in order, you can ensure the smooth operation of your network. Additionally, utilizing secondary name servers, such as those offered by One Avenue, provides the necessary redundancy to minimize service disruptions.

Ensuring these settings are correctly configured will result in a more reliable and efficient network, enhancing email deliverability and overall system performance.

Computer Requirements for BlueOnyx

Setting up a DNS and mail server using BlueOnyx is an efficient and effective way to manage your network services. BlueOnyx is versatile and can run on a wide range of hardware, making it accessible for various users. This article provides detailed information on the computer requirements necessary to run BlueOnyx effectively.

Minimum Hardware Requirements

- **CPU:** BlueOnyx can run on almost any computer or server that has a 64-bit CPU. This ensures compatibility with modern operating systems and applications.
- **Memory:** At a minimum, the system should have at least 2GB of memory. While this is sufficient for basic operations, more memory is recommended for better performance.
- **Storage:** A single new drive is required at the minimum. However, using two identical new drives is recommended to set up RAID 1 (mirrored drives). This configuration enhances data redundancy and reliability.

Recommended Hardware Specifications

- **Network Interface:** The system will need a network card or port to connect to your network. It is advisable to use a new cable to ensure the best possible connection.
- **Memory:** For optimal performance, especially if you plan to run antivirus software and applications like WordPress, it is recommended to have 16GB of memory. This allows the system to handle more processes simultaneously and improves overall efficiency.
- **Monitor and Keyboard:** A monitor and keyboard are necessary for the initial setup of BlueOnyx. These peripherals should be available for hands-on work as needed, such as troubleshooting or system maintenance.
- **Power Supply:** Dual power supplies are preferable, as they provide backup in case one fails. This redundancy helps ensure that your server remains operational even during power supply issues.

- **Boot Requirements:** Some versions of BlueOnyx may require a computer that can UEFI boot. Ensure that your hardware supports this feature if it is needed for the version you are installing.
- **Dedicated Server Systems:** Dedicated servers are preferred because they offer additional features such as CPU, drive, memory, and power redundancy. These systems are designed for continuous operation and provide greater reliability and performance for your DNS and mail server setup.

Advanced Considerations

- **Power Efficiency:** Newer systems generally use less power and generate less heat compared to older models. This can lead to cost savings on electricity and cooling, making them more environmentally friendly and economical in the long run.
- **Hardware Redundancy:** Utilizing newer dedicated server systems not only reduces power consumption but also often includes advanced features such as hot-swappable drives and modular components, which enhance the server's reliability and ease of maintenance.

Conclusion

When setting up a DNS and mail server using BlueOnyx, almost any modern computer or server with a 64-bit CPU, at least 2GB of memory, and a single new drive will suffice. However, for optimal performance, it is recommended to use a system with 16GB of memory, dual power supplies, and two identical drives configured in RAID 1. Ensuring that your system has a network card, a new network cable, and supports UEFI booting where required will help in smooth setup and operation.

Newer systems not only provide better performance but also use less power and produce less heat, making them ideal for a sustainable and efficient server environment. Most off-the-shelf computers are capable of running BlueOnyx, making it an accessible solution for those looking to manage their own DNS and mail servers effectively. By following these guidelines, you can ensure a robust and reliable setup that meets your needs.

Retrieving the BlueOnyx ISO

The ISO image for BlueOnyx can be downloaded from the official BlueOnyx updates repository. You can find the ISO at the following URL: http://updates.blueonyx.it/pub/BlueOnyx/ISO/. This ISO file is necessary to create the installation media.

Verifying the ISO File with MD5SUM on Windows

Before using the ISO file, it is important to verify its integrity by checking the MD5 checksum. This ensures that the file has not been corrupted during the download process.

1. Download the MD5 checksum file from the same directory where you downloaded the ISO.
2. On your Windows computer, download and install a tool like WinMD5Free.
3. Open WinMD5Free and select the downloaded ISO file.
4. The tool will generate an MD5 checksum for the ISO. Compare this value with the one provided in the MD5 checksum file.
5. If the values match, the ISO file is intact and ready to use. If they do not match, download the ISO file again.

Creating Installation Media

Burning the ISO to a USB Drive

Creating a bootable USB drive is a convenient way to install BlueOnyx. Here are the steps:

1. Download and install a tool like Rufus from https://rufus.ie/.
2. Insert a USB drive into your computer.
3. Open Rufus and select the USB drive from the device list.
4. Click the “Select” button and choose the BlueOnyx ISO file.
5. Click “Start” to begin the process. Rufus will format the USB drive and copy the ISO contents, making it bootable.

Creating a Bootable DVD

If you prefer to use a DVD for installation, follow these steps:

1. Ensure you have a blank DVD with at least 2GB of storage.
2. Download and install a DVD burning tool like ImgBurn from http://www.imgburn.com/.
3. Open ImgBurn and select “Write image file to disc.”
4. Choose the BlueOnyx ISO file as the source and select your DVD drive as the destination.
5. Click the “Write” button to start burning the ISO file to the DVD.

Installation verification process

BlueOnyx will automatically verify the installation media when the install process starts; however, this is different than checking the MD5SUM of the ISO. Pressing ESC will abort the installation verification process if desired.

Verifying the integrity of the ISO file ensures a smooth installation process, and creating reliable installation media, whether on a USB drive or DVD, will facilitate the setup. By following these steps, you will be well-prepared to install BlueOnyx on your chosen hardware and enjoy the benefits of a secure, private, and reliable email server.

Conclusion

BlueOnyx will automatically verify the installation media when the install process starts; however, this is different than checking the MD5SUM of the ISO. Pressing ESC will abort the installation verification process if desired.

By following these steps, you will be well-prepared to install BlueOnyx on your chosen hardware. Verifying the integrity of the ISO file ensures a smooth installation process, and creating reliable installation media, whether on a USB drive or DVD, will facilitate the setup.

BlueOnyx's robust feature set and ease of use make it an excellent choice for managing web, email, and DNS services efficiently.

Installing BlueOnyx: A Step-by-Step Guide

Setting up a DNS and mail server using BlueOnyx is a straightforward process, but it requires careful attention to detail. This guide will walk you through the installation process to ensure a successful setup.

Booting from Installation Media

1. Insert Installation Media: Insert the bootable DVD or USB drive that you created in the preparation phase into the computer.
2. Boot from Media: Power on the computer and enter the BIOS or UEFI settings (usually by pressing a key like F2, F12, DEL, or ESC during startup). Set the boot priority to boot from the DVD or USB drive first. Save the changes and exit the BIOS/UEFI settings.

Installing BlueOnyx

3. Start Installation: The computer will boot from the installation media, and the BlueOnyx installer will start.
4. Data Deletion Warning: Be aware that this installation process will delete all data on the computer. Ensure that you have backed up any important data before proceeding.
5. Automatic Installation: When prompted, choose the first option, "Automatic Installation." This option will automatically partition the disk and install BlueOnyx.
6. Wait for Completion: The installation process will take some time. Wait until the installation is complete. Once done, the system will prompt you to reboot.
7. Reboot the System: Reboot the computer to start using the newly installed BlueOnyx system.

Initial Login and Network Configuration

8. Login as Root: After the reboot, you will be presented with a login screen. Login using the username “root” and the password “blueonyx.”

9. Network Settings Program: The network settings program will be displayed. Configure only the IPv4 settings with the IP information provided by your service provider. Do not configure IPv6 at this stage.

Completing the Setup

10. Access BlueOnyx via Browser: Open a web browser on another computer connected to the same network and navigate to the IP address you configured for the BlueOnyx server.
11. Nameserver Configuration: Enter the nameserver information provided by your service provider. This step is crucial for the proper resolution of domain names.
12. Save Configuration: Once you have completed all the required configuration tabs in the browser interface, click the “Save” button to apply the settings.
13. System Update: Go back to the terminal on the BlueOnyx server. Optionally, you may run a system update to ensure all packages are up to date. Execute the command: “yum update -y” After the update is complete, reboot the server using the “reboot” command

Final Steps

14. Verify the Setup: After the server reboots, it should be ready for site configuration. Ensure that you can ping the server and log in via the browser interface.
15. Site Configuration: Begin configuring your DNS and mail server settings as required for your specific use case.

Conclusion

By following these detailed steps, you will have successfully installed and configured BlueOnyx on your server. The system should now be ready for further configuration and use. With BlueOnyx, you have a powerful platform for managing DNS, mail, and web services, ensuring reliability and security for your network.

Installing BlueOnyx on VirtualBox and VMware

Setting up a DNS and mail server using BlueOnyx can be done on virtualized environments like VirtualBox and VMware. This article provides detailed instructions on how to set up BlueOnyx on these platforms, ensuring you understand the benefits and limitations of virtual environments for server use.

What is VirtualBox?

VirtualBox is an open-source virtualization software that allows you to run multiple operating systems simultaneously on a single physical machine. It is compatible with most operating systems, including Windows, macOS, Linux, and Solaris.

Downloading the BlueOnyx VDI for VirtualBox

For VirtualBox users, there is a VDI (Virtual Disk Image) available for download at http://updates.blueonyx.it/pub/BlueOnyx/OVA/. This VDI file contains a pre-configured BlueOnyx system, making the installation process straightforward.

System Requirements for VirtualBox

The VDI has the same system requirements as a hardware system:

- A 64-bit CPU
- At least 2GB of RAM (16GB is preferred if running additional services like antivirus or WordPress)
- A single or mirrored drives setup for storage
- A network card or port
- A monitor and keyboard for initial setup

Installing BlueOnyx on a Windows Computer Running VirtualBox

1. **Download and Install VirtualBox:** Visit the VirtualBox website and download the latest version for Windows. Install VirtualBox following the on-screen instructions.

2. **Download the VDI File:** Download the BlueOnyx VDI file from http://updates.blueonyx.it/pub/BlueOnyx/OVA/.

3. **Create a New Virtual Machine:**
   - Open VirtualBox and click on “New” to create a new virtual machine.
   - Name your VM (e.g., “BlueOnyx”) and select “Linux” as the type and “Other Linux (64-bit)” as the version.
   - Allocate at least 2GB of RAM (16GB is recommended for optimal performance).
   - Use the Existing VDI:
   - When asked for a hard disk, select “Use an existing virtual hard disk file” and browse to the location of the downloaded VDI file.

4. **Configure Network Settings:**
   - Go to the VM settings, select “Network,” and ensure the adapter is attached to “Bridged Adapter” to allow the VM to access the network.
   - Start the VM: Click “Start” to boot the BlueOnyx virtual machine. Follow the on-screen instructions to complete the setup.

Using BlueOnyx with VMware

For users who prefer VMware, a VMDK (Virtual Machine Disk) is available for download, which is compatible with VMware Workstation, VMware Player, and VMware ESXi.

Downloading the BlueOnyx VMDK for VMware

The VMDK file can be downloaded from the same URL: http://updates.blueonyx.it/pub/BlueOnyx/OVA/. This file allows you to deploy BlueOnyx on VMware environments.

Installing BlueOnyx on VMware

1. **Download and Install VMware:** Download and install the appropriate VMware product (Workstation, Player, or ESXi) for your system.
2. **Download the VMDK File:** Download the BlueOnyx VMDK file from http://updates.blueonyx.it/pub/BlueOnyx/OVA/.
3. **Create a New Virtual Machine:**
   - Open VMware and create a new virtual machine.
   - Select “Custom” configuration and choose “I will install the operating system later.”
4. **Use the Existing VMDK:**
   - When asked for a disk, select “Use an existing virtual disk” and browse to the location of the downloaded VMDK file.
5. **Configure Network Settings:**
   - Ensure the network adapter is set to “Bridged” mode for proper network connectivity.
6. **Start the VM:** Power on the virtual machine and follow the on-screen instructions to complete the BlueOnyx setup.

Conclusion

While setting up BlueOnyx on VirtualBox and VMware is feasible and convenient for testing or development purposes, it may not be the best choice for production environments. Virtualized systems may lack the reliability and performance required for a dedicated DNS and mail server.

For increased reliability and availability, it is recommended to use dedicated hardware systems. Dedicated systems offer better performance, stability, and security, making them more suitable for critical server operations.

By investing in dedicated hardware, you ensure that your DNS and mail servers are robust, reliable, and capable of handling the demands of your network infrastructure.

Starting the Basic Configuration of BlueOnyx

Once BlueOnyx is installed, it is essential to complete the basic configuration to ensure that your DNS and mail server functions correctly. Follow these detailed instructions to finalize the setup.

Accessing the BlueOnyx Interface

1. Go to the Main IP Address: Open a web browser and navigate to the main IP address of your BlueOnyx server.
2. Login: Enter the username “admin” and the password you created during the installation process.

Configuring DNS Settings

1. Navigate to DNS Settings:
   - Click on “Network Services” in the main menu.
   - Select “DNS” from the dropdown.

2. Enable DNS Server:
   - On the DNS settings page, find the option to enable the DNS server and turn it on.

Configure Advanced DNS Settings:

- Click on the “Advanced” tab within the DNS settings.
- Enable the following options:
  - Allow DNS Query Access
  - Allow Queries from Everyone
  - Allow DNS Cache Access
- In the “Zone Transfer Access by IP Address” text box, add the IP addresses of your secondary name servers. This allows these servers to receive zone transfers, ensuring they stay updated with the primary DNS server’s records.
- Click on “Save” to apply these settings.

AutoDNS Configuration:

- Return to the DNS settings and click on the “AutoDNS” tab.

- Note the hostnames listed in the top text box. These should be the names of your DNS servers.
- In the second text box, enter “mail”. This configuration allows your website to be hosted on a different server while this server handles email and DNS services.
- Click on “Save” to confirm the changes.

Reviewing Server Access

Check SSH Settings:

- Click on “Server Access” in the main menu.
- Verify if SSH (Secure Shell) is enabled. SSH is used for remote terminal sessions, which are critical for managing the server remotely.
- It is recommended to disable SSH when not in use to enhance security. However, note that SSH serves as an emergency access method for technical support.

Configuring System Settings

Set Time and Timezone:

- Click on “System Settings” in the main menu.
- Select “Time” from the options.
- Verify the timezone setting or update it to your current timezone.
- Click on “Save” to apply the changes.
- The Network Time Protocol (NTP) will keep the server’s time synchronized with global time standards.

Conclusion

By following these steps, you will complete the basic configuration of your BlueOnyx DNS and mail server. Ensuring that DNS settings are properly configured, reviewing server access settings, and maintaining accurate system time are critical steps in setting up a reliable and secure server environment. After completing these configurations, your server should be ready for site setup and operational use.

Adding a new Virtual Host

Setting up a virtual host is a crucial step in managing your DNS and mail server using BlueOnyx. Follow these detailed instructions to add and configure a virtual host.

Accessing the Virtual Host Configuration

1. Login to BlueOnyx: Open a web browser and navigate to the main IP address of your BlueOnyx server. Login using the username “admin” and the password you created during the installation process.

2. Navigate to Site Management:
   - Click on “Site Management” in the main menu.
   - Click on the “Add” button to add a new site.

Configuring the Virtual Host

IP Addresses:
- For “IPv4 IP Address,” enter the main IP address of your server.
- For “IPv6 IP Address,” enter the main IPv6 address if you have one (this is optional).

Host Name:
- Decide whether this site will be used primarily for web services or email. If the site will serve mail, use “mail” as the host name (e.g., mail.example.com). If it will serve both web and mail, use “www” as the host name (e.g., www.example.com).

Domain Name:
- Enter the domain name you are going to use (e.g., example.com) in the “Domain Name” text box.

Owner:
- By default, the “Owner” should be set to “admin.” This can be changed if you set up administrators for different groups of virtual hosts, but it is recommended to leave it as “admin” for now.

Site Prefix:

- The “Site Prefix” is optional and primarily used for organizational reasons. It can be left blank for basic setups.

Web Server Aliases:

- If this is a mail server, leave the “Web Server Aliases” text box blank.
- If this is a web server, enter your domain name (e.g., example.com).

Web Alias Redirects:

- This feature is for web development, allowing multiple domain names to be served from the same folder while keeping the client's URL bar displaying the server alias host/domain name.

Disable Email for Domain:

- Only under rare conditions should “Disable Email for Domain” be turned on. This should be left off when building a mail server.

Email Server Aliases:

- Enter the domain name (e.g., example.com) in the “Email Server Aliases” text box, usually regardless of whether the site will be a web or email server.

Catch-All Email Address:

- This is optional and can be used to catch emails not directed to an active email account. For example, if an employee leaves and their account is deleted, mail directed to them in the future will automatically go to the recipient listed in this text box.

Maximum Allowed Disk Space:

- Set this to a reasonable amount based on the number of users, website space, and leaving room for backups. You may set it to all available space but consider the needs of each user and overall server capacity.

Maximum Allowed Number of Users:

- Best practice is to set this to the number of users needed in production. This prevents unauthorized creation of new users without server admin access.

Automatic DNS Configuration:

- We will use this to create only the basic records needed for the domain. Future adjustments to these records can be done manually.

Preview Site Configuration:

- This feature allows the site configuration to be previewed before DNS propagation. Generally, this should be kept off.

Advanced Configuration Tab

- By clicking on the 'Advanced' tab, you will be presented with the following options that you should review to meet your needs.

Enable PHP Scripting:

- If you intend to use the site for websites or webmail systems, enable “PHP Scripting.” If this is a mail server only, you may leave it off.

MariaDB User and Database:

- This information is used for websites or webmail programs. It is not required for mail-only servers.

Enable Common Gateway Interface (CGI):

- This dates back to the early days of web development and can be safely left off in most cases.

Enable Server-Side Includes (SSI):

- Like CGI, this is an older feature and can be left off in most cases.

Enable SSL:

- Enable SSL if you plan to have an SSL website or webmail website. Note that this is not required for a mail server but may be necessary for secure web communications. BlueOnyx can maintain free certificates from Let’s Encrypt, and paid certificates are available from One Avenue and other providers.

Logs Enabled:

- Enable logging for the site. This should be left on for both security and to monitor server activity.

Allow User(s) Access to FTP:

- Enable this when and if your web developer needs to use FTP.

Redirect/Proxy Website:

- This is not required for normal mail or web server operation and should be left off.

Shell Access:

- By default, users should have no access or “NONE.” Web developers may need these advanced features, but they should be carefully guarded.

Two-Factor-Auth (2FA):

- 2FA for the control panel and shell access can be enabled after site creation and can be left off until then.

Enable Sub Domains:

- Enable this only if you want to create subdomains under this virtual host (e.g., one.example.com, two.example.com).

Final Steps

Save the Advanced Configuration:

- Click on the “Save” button in the advanced tab to apply these settings.

Wait for Virtual Host Creation:

- Wait for BlueOnyx to create the virtual host. Once done, your new site configuration should be active.

Conclusion

By following these detailed instructions, you will successfully add and configure a virtual host on your BlueOnyx server. Proper setup ensures reliable operation for your web and mail services, tailored to your specific needs.

Post-Creation Checks and Server Configurations

After creating a virtual host in BlueOnyx, there are several important checks and configurations that need to be completed to ensure that your DNS and mail server are functioning correctly. Follow these detailed instructions to finalize the setup.

Configuring DNS Records

1. **Accessing DNS Management:**
   - Login to the BlueOnyx admin interface by navigating to the main IP address of your server.
   - Click on “Server Management” in the main menu.
   - Select “Network Services” from the dropdown.
   - Click on “DNS” to access the DNS management settings.

2. **Editing Primary Services:**
   - Click on “Edit Primary Services.”
   - Select the server domain name from the pull-down list. This should be the domain you have configured (e.g., example.com).

3. **Adding Forward Address (A Record):**
   - Add a “Forward Address (A Record)” for ns1.example.com using the IP address associated with your domain.
   - If you have additional name servers (e.g., ns2.example.com, ns3.example.com), add forward address records for each of them.
   - Click “Save” to update the server with these records.

4. **Verification:**
   - Verify that you can access ns1.example.com in a browser. This confirms that the DNS settings are correctly configured and that the server is reachable.

Configuring SSL Certificates

Once your DNS is functioning correctly, the next step is to configure an SSL certificate for your server to ensure secure communications.

1. **Accessing SSL Management:**
   - Click on “Server Management” in the main menu.
   - Select “Security” from the dropdown.
   - Click on “SSL” to access the SSL management settings.

2. **Options for SSL Certificates:**
   - **Self-Generated Certificate:** You can create a self-generated certificate. Note that this certificate will not be accepted by browsers unless specifically allowed. This is generally not recommended for production environments.
   - **Create a Signing Request:** This option allows you to create a Certificate Signing Request (CSR) that you can use to purchase a certificate from a Certificate Authority (CA). This type of certificate is widely accepted by all browsers.
   - **Let’s Encrypt:** You can use Let’s Encrypt to obtain a free SSL certificate. Let’s Encrypt certificates are free and automatically renew, making them a convenient and secure choice. Note that Let’s Encrypt certificates have a shorter lifespan (90 days) compared to paid certificates (typically 1-2 years).

3. **Completing the Form:**
   - Before making a choice, complete the form with your server and domain details. This includes information such as your domain name, organization, and contact email.
   - After completing the form, select your preferred method for obtaining the SSL certificate.

Recommendations

- **Self-Generated Certificates:** Suitable for testing and development environments but not recommended for production due to trust issues.
- **Purchased Certificates:** Ideal for production environments where extended validation and browser trust are required.
- **Let’s Encrypt Certificates:** Recommended for most users due to their ease of use, automation, and widespread browser support. They offer the most frequent updates, ensuring your security settings are always current.

Final Steps

1. **Save Configuration:**
   - After setting up your SSL certificate, click on “Save” to apply the changes.

2. **Reboot if Necessary:**
   If prompted, reboot the server to ensure all configurations are properly applied.

3. **Verification:**
   - Once the server is back online, verify that the SSL certificate is correctly applied by accessing your domain via HTTPS (e.g., https://ns1.example.com).

Conclusion

By following these steps, you will have successfully completed the basic configuration and verification for your BlueOnyx DNS and mail server. Ensuring that DNS records are accurately configured and that your SSL certificates are in place is crucial for secure and reliable server operation. With these settings, your server will be ready to handle DNS queries and email services effectively.

Configuring DNS records and SSL certificates is essential for maintaining the security and reliability of your BlueOnyx server. Accurate DNS settings ensure that your domain is correctly routed and reachable, while SSL certificates protect your communications from unauthorized access.

Regularly verify your configurations to maintain optimal performance and security. This approach guarantees that your server operates smoothly, providing reliable and secure DNS and email services for your needs.

Securing eMail and Admin Panel Traffic with SSL

Configuring SSL certificates is a crucial step in securing both email communications and admin panel traffic on your BlueOnyx server. SSL (Secure Sockets Layer) certificates encrypt data transmitted between your server and clients, ensuring that sensitive information remains confidential and protected from unauthorized access. By setting up SSL certificates, you enhance security and build trust with your users by demonstrating a commitment to protecting their data.

Configuring SSL Certificates

1. **Accessing SSL Management:**
   - Click on “Server Management” in the main menu.
   - Select “Security” from the dropdown.
   - Click on “SSL” to access the SSL management settings.

2. **Options for SSL Certificates:**
   - Self-Generated Certificate: Create a self-signed certificate. This type of certificate will not be trusted by browsers without manual intervention but can be used for internal testing.
   - Create a Signing Request: Generate a Certificate Signing Request (CSR) to purchase a certificate from a trusted Certificate Authority (CA). This ensures wide acceptance across all browsers.
   - Let’s Encrypt: Use Let’s Encrypt to obtain a free SSL certificate. These certificates are widely accepted and renew automatically every 90 days, providing a balance between security and convenience.

3. **Completing the Form:**
   - Complete the required fields with your server and domain details, including your domain name, organization, and contact email.
   - Choose your preferred method for obtaining the SSL certificate (self-generated, CSR, or Let’s Encrypt).

4. **Generating the Certificate:**

- If you choose a self-generated certificate, follow the prompts to create it.
- If you choose to create a CSR, generate the request and follow the instructions from your chosen CA to complete the purchase.
- If you choose Let's Encrypt, click the appropriate button to initiate the certificate generation and installation process.

5. **Saving Configuration:**
   - After setting up your SSL certificate, click on "Save" to apply the changes.
   - Verify that the SSL certificate is correctly applied by accessing your domain via HTTPS (e.g., https://ns1.example.com).

Final Verification

1. **Verifying eMail and SSL:**
   - Verify that SSL is functioning correctly by sending a test email and checking the headers for the SSL connection.
   - Ensure that your SSL certificate is valid and properly configured by accessing your domain using HTTPS and checking for any certificate warnings.

Conclusion

By completing these configurations, you enhance the security, authenticity, and trustworthiness of your email and web communications. This provides a robust and reliable infrastructure for your DNS and mail server on BlueOnyx, ensuring that your communications are secure and compliant with best practices.

Additionally, configuring SSL certificates ensures that your data is encrypted and secure during transmission, protecting sensitive information and providing an added layer of trust.

Setting Up SPF Records in DNS

To ensure the proper setup of SPF (Sender Policy Framework) for your domain in BlueOnyx, follow these detailed instructions. SPF is a critical component for email authentication, helping to protect against email spoofing and phishing.

Understanding SPF Records: The Basics of SPF Records:

- SPF (Sender Policy Framework) records are used to specify which IP addresses are authorized to send emails on behalf of your domain. This helps prevent email spoofing.
- An SPF record is added as a TXT record in DNS and looks something like this: `v=spf1 ip4:<IPv4_address> ip6:<IPv6_address> -all`.
- To create a basic sample record replace `<IPv4_address>` and `<IPv6_address>` with your actual IP addresses. For example, if your IPv4 address is `192.0.2.1` and your IPv6 address is `2001:db8::1`, the record would look like this: v=spf1 ip4:192.0.2.1 ip6:2001:db8::1 -all

Accessing the DNS Settings

1. **Login to BlueOnyx:**
   - Open a web browser and navigate to the main IP address of your BlueOnyx server.
   - Login using the username “admin” and the password you created during the installation process.

2. **Navigate to DNS Settings:**
   - Click on “Server Management” in the main menu.
   - Select “Network Services” from the dropdown.
   - Click on “DNS” to access the DNS management settings.

3. **Selecting the Domain:**
   - Click on “Edit Primary Services”
   - If the domain you want to configure is not already selected, select it from the “select domain” drop down box.

4. **Add a TXT Record:**
    - Use the “Add a Record” drop-down box and select “Text (TXT) Record”.
    - This action will bring up the SPF record wizard.

Using the SPF Record Wizard

SPF Record Wizard:
- This wizard will guide you through the process of creating or editing an SPF record for your DNS domain.
- Host Name: (optional) Leave this blank unless you need a specific subdomain.
- Domain Name: Enter your domain name (e.g., example.com).
- Text Record: Enter the SPF record you created above.

Wizard Fields Explained:
- Your Domain: Your main domain name.
- Allow servers listed as MX to send email for this domain: Check this if your MX records should be allowed to send email.
- Allow current IP address of the domain to send email for this domain: Check this to allow the IP address of your domain.
- Allow any hostname ending in [domain] to send email for this domain: Check this if you want to allow subdomains to send email.
- IP addresses in CIDR format that deliver or relay mail for this domain: Enter any additional IP addresses in CIDR format.
- Add any other server hostname that may deliver or relay mail for this domain: Enter any other hostnames that should be allowed to send email.
- Any domains that may deliver or relay mail for this domain: Enter any other domains that should be allowed to send email.
- How strict should be the servers treating the emails?: Typically, you should select `-all` to specify that only the listed IP addresses are authorized.

5. **Adding the TXT Record:**
    - After filling out the form, copy the generated SPF record into the “Text Record” text box.

Saving the Configuration

6. **Save the DNS Record:**
   - Click on “Save” to add the new TXT record to your DNS configuration.

7. **Final Save:**
   - Click “Save” again to apply the changes to the server.

Conclusion

By following these detailed steps, you will have successfully added a SPF TXT record to your DNS configuration using BlueOnyx. This setup is crucial for ensuring the authenticity and security of your email communications. For complete details and further reading on SPF records, please refer to the [SPF record Homepage](http://www.openspf.org/).

Adding DKIM Records and Their Role in Email Security

Understanding DKIM Records and Their Role in Email Security

In the context of setting up a DNS and mail server using BlueOnyx, it is essential to understand DKIM (DomainKeys Identified Mail) records and how they enhance email security. DKIM is an email authentication method designed to ensure the integrity of emails by allowing the recipient to verify whether an email was altered during transit.

What are DKIM Records?

DKIM records use a pair of cryptographic keys: a private key and a public key. The private key is stored on your email server, while the public key is stored in your DNS as a TXT record. When an email is sent, the email server uses the private key to generate a digital signature that is added to the email's header. The receiving email server then retrieves the public key from the DNS and uses it to verify the signature. If the signature matches, it confirms that the email has not been altered and that it indeed originated from an authorized server for the domain.

History of DKIM

DKIM was developed as a joint effort by Yahoo!, Cisco, and other contributors. It was first proposed in 2004 and became an official standard with the publication of RFC 4871 in 2007. DKIM has since been widely adopted as a critical component of email security frameworks. For more detailed information, you can visit the official [DKIM website](http://www.dkim.org/).

Enhancing Security with DMARC

While DKIM operates silently, its effectiveness can be enhanced with DMARC (Domain-based Message Authentication, Reporting & Conformance) records. DMARC allows domain owners to specify how their emails should be handled if they fail DKIM or SPF (Sender Policy Framework) checks. By setting a DMARC policy, you can instruct receiving servers to reject, quarantine, or report emails that do not pass authentication checks. This adds an extra layer of security, ensuring that fraudulent emails are less likely to be delivered.

Configuring DKIM in BlueOnyx

Step-by-Step Instructions

1. **Login to BlueOnyx:**
   - Open a web browser and navigate to the main IP address of your BlueOnyx server.
   - Login using the username “admin” and the password you created during the installation process.

2. **Access Site Management:**
   - Click on “Site Management” in the main menu.

3. **Modify Virtual Site:**
   - Click on the modify icon (pencil icon) for the virtual site you want to create a DKIM record for.

4. **Navigate to Services:**
   - In the site settings, navigate to the “Services” section.

5. **Configure eMail Settings:**
   - Click on “eMail” to access the email settings.

6. **Enable OpenDKIM:**
   - Scroll down to the OpenDKIM section.
   - Turn on “Enable OpenDKIM” by clicking the checkbox.
   - Turn on “Create TXT Record” to automatically generate the necessary DKIM record in your DNS.

7. **Save Configuration:**
   - Click on “Save” at the bottom of the page to apply the changes.

Verifying DKIM Configuration

To verify that the new DKIM record is working, you can send a test email and check the email headers for the DKIM signature. Here’s how:

1. **Send a Test Email:**
   - Send an email from the configured domain to an external email account (such as Gmail or Yahoo).

2. **Check the Headers:**

- Open the received email and view its headers (most email clients have an option to view message source or headers).
- Look for the DKIM-Signature header. It should indicate that the email was signed using your domain's DKIM key.

3. **Use Online Tools:**
- You can also use online DKIM verification tools, such as [DKIMValidator](https://www.dkimvalidator.com/), to check the DKIM status of your emails.

By following these steps, you can ensure that your DKIM configuration is correctly set up, enhancing the security and integrity of your email communications. This not only protects your domain's reputation but also helps prevent email spoofing and phishing attacks.

Setting Up a DMARC Record

Setting up a DMARC (Domain-based Message Authentication, Reporting, and Conformance) record is an important step in enhancing the security of your email domain. DMARC records help mail servers determine how to handle unauthenticated emails and provide a mechanism for monitoring email deliverability.

What is a DMARC Record?

DMARC records are DNS records that help protect your email domain from unauthorized use, such as phishing and email spoofing. A DMARC record specifies the policy for handling emails that fail SPF (Sender Policy Framework) and DKIM (DomainKeys Identified Mail) checks. It also provides options for sending reports about email delivery and authentication.

Components of a DMARC Record

- **Policy (p):** Specifies the policy for handling emails that fail authentication. Possible values are `none`, `quarantine`, and `reject`.
- **Aggregate Report (rua):** Email address to which aggregate reports are sent. These reports provide statistics on email authentication results.
- **Forensic Report (ruf):** Email address to which forensic reports are sent. These reports provide detailed information about each failed authentication.
- **Subdomain Policy (sp):** Specifies the policy for handling emails from subdomains.
- **Alignment Mode for DKIM (adkim):** Specifies the alignment mode for DKIM. Possible values are `r` (relaxed) and `s` (strict).
- **Failure Reporting Options (fo):** Specifies the failure reporting options. A value of `1` indicates that forensic reports should be sent if either SPF or DKIM fails.

Example DMARC Record

Here is a sample DMARC record with reporting and tagging:

"v=DMARC1; p=quarantine; rua=mailto:abuse@example.com; ruf=mailto:abuse@example.com; sp=quarantine; adkim=s; fo=1;"

Adding a DMARC Record in BlueOnyx

1. **Access the Command Line:**
   - You will need to access the command line interface of your BlueOnyx server to add a DMARC record.

2. **Navigate to the DNS Zone File:**
   - DMARC records can only be added by editing the domain's special include zone file located in `/var/named/chroot/var/named/`.
   - Use the following command to edit the zone file:

   nano /var/named/chroot/var/named/db.example.com.include
   Replace `example.com` with your actual domain name.

3. **Add the DMARC Record:**
   - Add the following line to the zone file to create the DMARC record:

   _dmarc.example.com. IN TXT "v=DMARC1; p=quarantine; rua=mailto:abuse@example.com; ruf=mailto:abuse@example.com; sp=quarantine; adkim=s; fo=1;"

   Adjust the values according to your specific requirements.

4. **Update the DNS Serial:**
   - The domain's DNS serial number must be updated for these changes to take effect. This can be done by adding a temporary DNS record, saving it, and then deleting it to trick the system into recognizing the changes.
   - For example, add a random A record:
     temporary.example.com. IN A 127.0.0.1

   Save the changes, then delete this temporary record.

5. **Save and Exit:**
   - Save the changes to the zone file and exit the text editor (in `nano`, you can do this by pressing `Ctrl+X`, then `Y`, and `Enter`).

Monitoring and More Information

- Reporting Email Address: Ensure the email addresses specified in `rua` and `ruf` are monitored regularly to receive aggregate and forensic reports.
- DMARC.org: For more details on DMARC and its configuration, visit the official website at [DMARC.org](https://dmarc.org/).

Conclusion

By following these detailed steps, you will have successfully added a DMARC record to your DNS configuration in BlueOnyx. This setup will help improve the security of your email domain by specifying policies for handling unauthenticated emails and providing mechanisms for monitoring email deliverability.

Setting Up SSL for Websites

Setting up an SSL certificate for your public website or webmail system is crucial for securing communications and building trust with your users. Follow these detailed instructions to enable SSL on your virtual host in BlueOnyx.

Enabling SSL for the Virtual Host

1. **Login to BlueOnyx:**
   - Open a web browser and navigate to the main IP address of your BlueOnyx server.
   - Login using the username “admin” and the password you created during the installation process.

2. **Navigate to Virtual Host Settings:**
   - Click on “Site Management” in the main menu.
   - Locate the virtual host you wish to configure and click on the settings “pencil icon” next to it to access its configuration.

3. **Enable SSL:**
   - In the virtual host settings, navigate to the “Advanced” tab.
   - Enable the “Enable SSL” checkbox. This allows the virtual host to serve a secure SSL website or webmail website.
   - Note that SSL is not required for a mail server and should only be enabled if needed for web services.

Choosing the Type of SSL Certificate

4. **Options for SSL Certificates:**
   - Self-Generated Certificate: This option creates a self-signed certificate, which will not be trusted by browsers unless specifically allowed. Suitable for internal testing but not recommended for public websites.
   - Create a Signing Request: This option generates a Certificate Signing Request (CSR) that you can use to purchase a certificate from a trusted Certificate Authority (CA). This ensures the certificate is widely accepted by all browsers.

- Let's Encrypt: This option allows you to obtain a free SSL certificate from Let's Encrypt. These certificates are trusted by most browsers and are automatically renewed every 90 days.

5. **Considerations for SSL Certificates:**
   - Self-Generated Certificates: These are valid for a limited period and need to be manually trusted by users. Not ideal for public-facing services.
   - Purchased Certificates: These typically have longer validity (1-2 years) and provide extended validation options.
   - Let's Encrypt Certificates: Free and automatically renewed, providing a convenient and secure choice for most users.

Requesting a Free SSL Certificate from Let's Encrypt

6. **Using Let's Encrypt:**
   - In the SSL configuration page, click on the "Let's Encrypt" button.
   - Fill out the form with your server and domain details, including your email address for renewal notifications.

7. **Enable Certificate Request and Renewal:**
   - Enable the checkbox for "Request or Renew Certificate."
   - For best results, enable auto-renewal and set a renewal period that provides sufficient time for technical support to address any issues before the certificate expires. A recommended period is 69 days.

8. **Save Configuration:**
   - Click on "Save" to apply the changes and request the SSL certificate from Let's Encrypt.

9. **Verify SSL Configuration:**
   - Once the SSL certificate is issued and installed, verify that your website is accessible via HTTPS by navigating to your domain (e.g., https://www.example.com).

- Check for the padlock icon in the browser's address bar, indicating a secure connection.

Conclusion

By following these steps, you will have successfully set up an SSL certificate for your public website or webmail system using BlueOnyx. Ensuring that SSL is enabled and properly configured enhances the security of your communications and builds trust with your users.

Whether you choose a self-generated certificate, a purchased certificate, or a free Let's Encrypt certificate, each option provides a different level of convenience and trust, allowing you to select the best fit for your needs.

Adding Users and eMail Aliases

Setting up users in BlueOnyx is an essential part of managing your DNS and mail server. Follow these detailed instructions to add and configure users for your domain.

Accessing User Management

1. **Login to BlueOnyx:**
   - Open a web browser and navigate to the main IP address of your BlueOnyx server.
   - Login using the username “admin” and the password you created during the installation process.

2. **Navigate to Site Management:**
   - Click on “Site Management” in the main menu.
   - Locate the domain you wish to manage and click on the settings “pencil icon” next to it to modify the domain.

3. **User List:**
   - You should be presented with the user list if there are any existing users. To add a new user, click on the “Add” button.

Adding a New User

4. **Full Name:**
   - Enter the user’s name in the “Full Name” text box.

5. **Username:**
   - Choose a username for the new user. This username will also serve as an active email address (e.g., username@example.com).
   - The user can later be assigned additional addresses, such as “accounting@example.com”. You can use non-user-related names like “a7s3ioe” to represent specific roles, such as “attorney seven’s secretary number three’s inter-office email”.

6. **Password:**
   - Enter a strong password in the password fields to ensure security.

7. **Maximum Allowed Disk Space:**
    - The disk space used by this user is based on the maximum disk space assigned to the virtual host.
    - Assign a lower limit to manage space effectively and to catch problems such as users not deleting spam, storing large archives of sent or deleted mail, or maintaining huge folders on the server. This helps in managing backup sizes and extends drive longevity.

8. **Shell Access:**
    - Shell access is not recommended for regular users and should be limited to website administrators as needed.
    - Set “Shell Access” to “none” for regular users.

9. **Two-Factor Authentication (2FA):**
    - 2FA is designed for users with control panel and/or shell access for added security.
    - Enable 2FA if you want to use it for enhanced security.

10. **Site Administrator:**
    - If enabled, the user has the ability to login to the control panel and manage website files.

11. **DNS Administrator:**
    - If enabled, the user has the ability to login to the control panel as a “DNS Administrator” for the virtual host’s domains.

12. **Disable User's Email:**
    - If, for some reason, you want to create a user without email service, you can enable “Disable User's Email”.

13. **Email Aliases:**
    - This is where you can add email aliases for the user. Examples include “accounting”, “marketing”, “computers”, “legal”, and “abuse”.

14. **Remarks:**
    - Additional “Remarks” are optional and can be used for any extra information you want to store about the user.

15. **Save the User:**
    - Click on “Save” to add the new user.

Additional User Management

16. **Setup Additional Users:**
    - Repeat the above steps to set up additional users as needed.

17. **Adjust Maximum Users:**
    - After adding users, you may want to adjust the site’s maximum number of users to accommodate future additions.

Conclusion

By following these steps, you will have successfully added and configured users for your domain in BlueOnyx. Proper user management ensures efficient operation of your DNS and mail server, helping to maintain security and organization. Adjust the site’s settings as necessary to fit your specific requirements.

Configuring an Email Client

Setting up an email client for use with your BlueOnyx mail server involves configuring the incoming and outgoing mail servers, understanding the differences between TLS and SSL, and setting the correct ports. Additionally, configuring SRV records can help certain email clients like Outlook automatically detect and configure the mail server settings.

Incoming and Outgoing Mail Servers

1. **Incoming Mail Server:**
   - The incoming mail server is typically configured to use either IMAP or POP3 protocols.
   - For IMAP, the server address will usually be `mail.example.com` (replace `example.com` with your actual domain).
   - For POP3, the server address will be the same, `mail.example.com`.

2. **Outgoing Mail Server:**
   - The outgoing mail server uses the SMTP protocol.
   - The server address for SMTP will also be `mail.example.com`.
   - Authentication using ‘username’ and ‘password’ is required by default.

Understanding TLS and SSL

TLS (Transport Layer Security):
- TLS is a security protocol that provides encryption for email communications.
- Unlike SSL, TLS does not require a certificate for the client side, but it uses the server's certificate to establish a secure connection.
- It is recommended to use TLS for secure email communications as it is more secure and up-to-date compared to SSL.

SSL (Secure Sockets Layer):
- SSL is an older security protocol that also provides encryption.
- SSL requires a certificate to establish a secure connection.

- Although SSL is still widely used, it is recommended to use TLS due to its enhanced security features.

Ports available to Use

1. IMAP (with TLS): Port 143
2. IMAP (with SSL): Port 993
3. POP3 (with TLS): Port 110
4. POP3 (with SSL): Port 995
5. SMTP (with TLS): Port 25 or 587
6. SMTP (with SSL): Port 465

General Configuration for Clients

- **Incoming Mail Server (IMAP/POP3):** Set to `mail.example.com`. Ensure you configure SSL/TLS for securing incoming mail connections. Use port 993 for IMAP or 995 for POP3 when SSL/TLS is enabled.
- **Outgoing Mail Server (SMTP):** Set to `mail.example.com`. Use TLS/SSL to secure SMTP connections. Typically, port 587 is used for SMTP with STARTTLS, or port 465 for SMTPS (SMTP over SSL). Use authentication.

Usernames and Email Addresses

1. **Username Format:**
   - Usernames in BlueOnyx do not include the domain name and are structured like email addresses (e.g., `username@example.com`).
   - Aliases cannot be used as usernames.

2. **Dovecot Configuration:**
   - Dovecot can be configured to accept `username@example.com` format by setting `auth_username_format = %Ln` in `/etc/dovecot/conf.d/10-auth.conf`. Outlook may require this when adding new accounts

SRV Records for Mail Clients

1. **Understanding SRV Records:**

- SRV records are DNS records used to define the location (hostname and port) of servers for specified services.
- Email clients like Outlook may use SRV records to automatically detect mail server settings.

2. **Adding SRV Records:**
   - SRV records can only be added using the command line and by editing the domain's special include zone file located in `/var/named/chroot/var/named/`.
   - Use a command like `nano /var/named/chroot/var/named/db.example.com.include` to edit the file.

3. **Updating DNS Serial:**
   - The domain's DNS serial must be updated for these changes to take effect.
   - This involves tricking the system by adding a temporary DNS record (like a random A record), saving it, and then deleting it.

Sample SRV Records

pri.example.com._autodiscover._tcp.example.com. IN SRV 0 0 993 mail.example.com.

pri.example.com._smtp._tcp.example.com. 3600 IN SRV 10 0 25 mail.example.com.

pri.example.com._smtps._tcp.example.com. 3600 IN SRV 10 0 465 mail.example.com.

pri.example.com._imap._tcp.example.com. 3600 IN SRV 10 0 143 mail.example.com.

pri.example.com._imaps._tcp.example.com. 3600 IN SRV 10 0 993 mail.example.com.

pri.example.com._pop3._tcp.example.com. 3600 IN SRV 10 0 110 mail.example.com.

pri.example.com._pop3s._tcp.example.com. 3600 IN SRV 10 0 995 mail.example.com.

pri.example.com._ftp._tcp.example.com. 3600 IN SRV 10 0 21 mail.example.com.

pri.example.com._ftps._tcp.example.com. 3600 IN SRV 10 0 990 mail.example.com.

Conclusion

By following these steps, you will be able to set up an email client to work with your BlueOnyx mail server, ensuring secure and efficient email communication. Proper configuration of SRV records can enhance the setup process, especially for clients like Outlook. Make sure to use strong passwords and enable TLS for the best security practices.

Optional old fashioned PoprelayD

To allow IPs to send mail automatically after successfully checking their mail for a specified period, you will need to configure your BlueOnyx server to use Sendmail instead of the default Postfix. This configuration enables POP before SMTP authentication, commonly referred to as POP before relay.

This setup allows IPs to send mail automatically after successfully checking their mail, accommodating email clients that do not support SMTP authentication when sending mail. It ensures that users can send emails seamlessly after authenticating via POP, which was a common method for older email clients.

Changing from Postfix to Sendmail and turning on PopRelayD

1. 1. **Login to BlueOnyx:**
   - Open a web browser and navigate to the main IP address of your BlueOnyx server.
   - Login using the username “admin” and the password you created during the installation process.
2. **Navigate to Email Advanced Settings:**
   - Click on “Server Management” in the main menu.
   - Select “Network Services” from the dropdown.
   - Click on “eMail” to access the email settings.
   - Once on the email settings page, click on the “Advanced” tab.
   - The first dropdown menu on this page allows you to choose between Postfix and Sendmail.
   - Select “Sendmail” from the dropdown menu.
   - Scroll down and click on “Save” at the bottom of the page to apply the changes.
   - After the page refreshes, you will see additional options now that Sendmail is enabled.
   - Look for the option to enable “POP before relay.”
   - Enable this option by clicking the checkbox next to it.
   - Scroll down and click on “Save” again to apply this setting.

WARNING: PopRelayD was removed from Sendmail on March 1, 2000, and has been recreated here to support legacy users. Its usage should be avoided due to potential denial of service attacks and unauthorized sending by other users or applications. These risks occur because the client's IP remains authorized for a period of time after checking for new email and the rebuilding of the allowed senders database process failing.

Web Development with BlueOnyx

Web development and hosting have been integral components of BlueOnyx for over 20 years. The platform offers a robust and versatile environment for web developers, providing support for various backend technologies and protocols to facilitate comprehensive web hosting solutions.

Supported Backend Software

BlueOnyx supports a wide array of backend software, making it a powerful platform for web development:

- **Perl:** A high-level programming language known for its capabilities in text manipulation and its extensive library of third-party modules.
- **PHP:** A popular server-side scripting language used for web development, enabling the creation of dynamic web pages and applications.
- **MySQL:** An open-source relational database management system, essential for storing and managing data for dynamic websites.
- **Operating System:** BlueOnyx is RPM-based and currently supports AlmaLinux and Rocky Linux, both of which are clones of RedHat 9. Historically, BlueOnyx has supported every version of CentOS, demonstrating its long-standing reliability and adaptability.

Access for Web Developers

Web developers may access the server using various protocols, provided they are authorized in the control panel and the protocols are enabled for the site and the server:

- **FTP:** File Transfer Protocol for uploading and downloading files to and from the server.
- **SSH:** Secure Shell for secure remote command-line access and execution of commands on the server.
- **SFTP:** Secure File Transfer Protocol, which uses SSH to secure the transfer of files.
- **SCP:** Secure Copy Protocol, also based on SSH, for securely transferring files between hosts.

Site Admin Access

To perform web development tasks on BlueOnyx, developers need to have “site admin” level access. This level of access provides the necessary permissions to manage and modify the website files and settings.

File Storage Locations

Website files are stored in specific directories based on their configuration as a web server or a mail server:

- For websites configured as web servers, files are stored in: `/home/sites/www.example.com/wwwroot/web`
- For sites configured as mail servers, files are stored in: `/home/sites/mail.example.com/wwwroot/web`

Replace `example.com` with your actual domain name.

Conclusion

BlueOnyx provides a rich and versatile environment for web development, supporting a wide range of backend technologies and protocols. By ensuring developers have the appropriate access levels and understanding where files are stored, they can effectively manage and develop websites on the BlueOnyx platform.

This robust system, with its support of modern Linux distributions like AlmaLinux and Rocky Linux, ensures a reliable and powerful hosting solution for web developers.

Adding a Server Administrator for Enhanced Security

Adding a server administrator in BlueOnyx is an effective way to enhance security by assigning specific roles and permissions to different users. This ensures that each administrator has access only to the virtual hosts they are responsible for, thereby limiting the potential for unauthorized access to sensitive email accounts and related files.

Example Scenario

Imagine you have multiple virtual hosts under one main account owned by the admin, such as `mail.example.com`, `www.example.com`, and `ten.example.com`. You may want to limit access to `mail.example.com` to only the main administrator while giving full access to `ten.example.com` to a hired employee or contractor. By creating a dedicated administrator account for them and assigning the relevant virtual hosts, you can control and limit access effectively.

Steps to Add a Server Administrator

1. **Login to BlueOnyx:**
   - Open a web browser and navigate to the main IP address of your BlueOnyx server.
   - Login using the username “admin” and the password you created during the installation process.

2. **Navigate to Server Administrator:**
   - From the main menu, click on “Server Administrator.”

3. **Add a New Administrator:**
   - Click on the “Add” button to create a new administrator account.

4. **Enter Administrator Details:**
   - Name: Enter a name or reference name for the new administrator. This could be the name of the person or a reference that indicates their role or responsibility.
   - Username: Use a secure and unique username for the new administrator. This should not be easily guessable.

- Password: Enter a strong password to ensure the security of the account. The password should be complex, including a mix of letters, numbers, and special characters.

5. **Configuring Options:**
   The rest of the options depend on your specific use case and should be completed according to your needs. These may include:
   - Assigning specific virtual hosts to the administrator.
   - Setting permissions and access levels.
   - Configuring additional security settings.

Assigning Virtual Hosts

By assigning specific virtual hosts to the new administrator, you can limit their access to only those domains they are responsible for. For instance, if the new administrator is hired to manage `ten.example.com`, you would assign this virtual host to their account while restricting access to `mail.example.com` and `www.example.com`.

Example Configuration

- Account Name: Jane Doe
- Username: janedoe_admin
- Password: [Strong password]
- Assigned Virtual Hosts: `ten.example.com`
- Permissions: Full access to `ten.example.com`

Conclusion

By carefully setting up server administrators in BlueOnyx, you can enhance the security and management of your virtual hosts. This approach ensures that each administrator has access only to the domains they are responsible for, reducing the risk of unauthorized access to sensitive email accounts and related files.

Following these detailed steps will help you create a secure and organized administrative structure for your BlueOnyx server.

Configuring an eMail Relay Server

Setting up a mail server relay can help distribute the load of incoming emails and provide redundancy, ensuring that your email services remain reliable and efficient. Follow these detailed instructions to set up a mail server relay using BlueOnyx.

Step 1: Create or Install Another Server

1. **Create or Install a New BlueOnyx Server:**
   - Follow the previous instructions for installing BlueOnyx on a new server. Note that there is no need to add a virtual host on this server since it will be used solely as a mail relay.

Step 2: Configuring the Relay Server

1. **Access Network Services:**
   - Login to the new BlueOnyx server using the admin credentials.
   - Navigate to the main menu and click on “Network Services”.

2. **Configure Email Settings:**
   - Click on “eMail” in the Network Services menu.
   - Select the “Secondary Mail-server” tab.
   - Click on “Add” to add a new relay configuration.

3. **Enter Domain Information:**
   - In the “Domain Name” field, enter the domain you want to relay for, such as `example.com`.
   - The “Primary Mail Server” is the server that will ultimately receive and store the emails. This is where users will check their emails.
   - Enter the IP address of the primary mail server in the appropriate field.
   - Click “Save” to apply the settings.

Step 3: Setting Up DNS for the New Relay Server

1. 1. DNS Configuration:

- Return to your primary DNS server and log in.
- Navigate to the DNS settings for the domain you are configuring (e.g., `example.com`).

2. **Understanding MX Records:**
   - Mail Exchanger (MX) records in DNS specify the mail servers responsible for receiving email on behalf of a domain. MX records are prioritized using numerical values, where lower values have higher priority.
   - For example, using priorities 10, 30, and 50 would designate the primary, secondary, and tertiary mail servers, respectively.

3. **Configure MX Records:**
   - - Set the MX record for the primary mail server to 10.
   - - Set the MX record for the new relay server to 30.
   - - If you have additional mail servers, you can set their MX records to 50 or higher.
   - - Remember, using an MX record priority of 0 will cause all emails to go only to that server.

Example DNS Configuration

Here is an example configuration for your DNS MX records:

```
example.com.  IN  MX  10  mail.example.com.
example.com.  IN  MX  30  relay.example.com.
```

Replace `mail.example.com` and `relay.example.com` with the actual hostnames or IP addresses of your primary and relay servers.

Final Steps

1. **Verify Settings:**
   - Ensure that the settings are correctly applied and that both the primary and relay servers are configured properly.

- Test the email relay setup by sending test emails to the domain and verifying that they are correctly routed through the relay server to the primary mail server.

2. **Monitoring and Maintenance:**
   - Regularly monitor the performance and logs of both servers to ensure they are functioning correctly.
   - Update the DNS records as needed if there are any changes to the server configurations or IP addresses.

Conclusion

By setting up a mail server relay in BlueOnyx, you enhance the reliability and efficiency of your email services. Following these detailed steps will help you configure the relay server and ensure that your DNS settings are correctly applied, providing a robust and resilient email infrastructure.

Using the Active Monitor: Understanding and Configuring

In the context of setting up a DNS and mail server using BlueOnyx, it is essential to leverage the built-in service monitoring system known as “Active Monitor.” This system is designed to ensure the continuous operation of selected services, enhancing the reliability and stability of your server. Here’s a detailed explanation of how the Active Monitor works and how you can configure it to meet your needs.

What is the Active Monitor?

The “Active Monitor” in BlueOnyx is a robust service monitoring system that continuously checks to ensure selected services are running smoothly. It operates by performing simple tests every 15 minutes to verify the functionality of various services. If any issues are detected, the Active Monitor attempts to resolve them by restarting the affected service. This proactive approach helps maintain optimal server performance with minimal downtime.

How Does the Active Monitor Notify You?

When the Active Monitor detects a problem, it will automatically send an email notification to the admin account. However, you can specify a different email address in the “Active Monitor” settings to receive these alerts. This flexibility allows you to ensure that critical notifications are directed to the appropriate personnel, helping you to address issues promptly.

Configuring Active Monitor in BlueOnyx

To configure the Active Monitor, follow these steps:

1. **Access Active Monitor Settings:**
   - Login to the BlueOnyx admin interface by navigating to the main IP address of your server.
   - Click on “Server Management” in the main menu.
   - Select “Active Monitor” from the dropdown menu.
   - Click on “Settings” to access the Active Monitor configuration page.

2. Setting the Alert Email Address:

- In the “Active Monitor Settings” section, you will find an option to specify the alert email address.
- Enter the email address where you want to receive notifications about service issues.
- Click “Save” to apply the changes.

3. Enabling or Disabling Monitoring:

- Within the “Active Monitor Settings” section, you can choose to enable or disable monitoring for the entire system.
- This toggle allows you to manage whether the Active Monitor is actively checking your services.

4. Selecting Monitored Components:

- Click on “Monitored Components” to view and configure the list of services that the Active Monitor checks.
- You can select or deselect services based on your specific needs and preferences.
- Ensure that critical services such as DNS, email, and web server components are included in the monitored list to maintain system integrity.

How Active Monitor Enhances Your Server Management

By default, the Active Monitor sends email notifications to the admin account whenever an event occurs, such as a service failure or restart. This alert system is crucial for keeping server operators informed about the health and status of their services.

The ability to customize which services are monitored and where alerts are sent provides a high level of control and flexibility, ensuring that you can tailor the monitoring system to fit your operational requirements.

Benefits of Using Active Monitor

- **Proactive Problem Resolution:** The Active Monitor not only detects issues but also attempts to restart failed services automatically, minimizing downtime.
- **Customizable Alerts:** Notifications can be sent to any specified email address, ensuring that alerts reach the right individuals promptly.
- **Comprehensive Monitoring:** By selecting critical components for monitoring, you can ensure that your essential services are always up and running.
- **Ease of Configuration:** The intuitive interface allows you to quickly configure and manage the monitoring settings, making it easy to maintain optimal server performance.

Conclusion

The Active Monitor system in BlueOnyx is a powerful tool for ensuring the reliability and stability of your server. By configuring the Active Monitor to check critical services and notify you of any issues, you can maintain continuous operation and promptly address any problems that arise.

This proactive monitoring solution is essential for maintaining a secure and efficient server environment, giving you peace of mind that your services are running smoothly and reliably.

The Importance of Monitoring Email Operation

Ensuring the proper operation of your email server is critical for maintaining reliable communication. Effective monitoring can help identify issues promptly, allowing for quick resolution. Here are some detailed recommendations for monitoring your email system to ensure its proper operation.

Importance of Monitoring

Monitoring your email system is essential to detect and resolve issues before they impact your users. This proactive approach helps maintain the reliability and integrity of your communication infrastructure.

How Monitoring Works

1. **Automated Test Messages:**
   - Monitoring systems can be configured to send a test message every 5 minutes.
   - These test messages simulate the actions of a typical user, ensuring that the email server is capable of receiving emails consistently.

2. **Verification Process:**
   - After sending a test message, the monitoring system checks to see if the server has received the email.
   - If the server fails to receive the email, the monitoring system triggers an alert.

3. **Alert Mechanisms:**
   - Alerts can be sent via email, text message, or phone call.
   - Alerts notify you of any issues with the email server, allowing for timely intervention and resolution.
   - Phone calls as alerts may incur an additional fee, providing an immediate and direct notification method.

Monitoring Services Offered by One Avenue

1. **In-House Monitoring:**

- One Avenue offers in-house email monitoring services that utilize automated systems to ensure your email server is functioning correctly.
- In-house monitoring integrates seamlessly with your BlueOnyx setup, providing customized solutions tailored to your needs.

2. **Third-Party Monitoring:**
   - In addition to in-house services, One Avenue also supports third-party monitoring systems.
   - Third-party monitoring can provide additional layers of redundancy and verification, ensuring that your email system remains robust and reliable.

Service Requirements

1. **User Account for Monitoring:**
   - Monitoring services require a user account that can be supplied to One Avenue and third-party providers.
   - This user account is used to send and receive test messages, allowing the monitoring system to verify the proper operation of the email server.
2. **Configuration and Setup:**
   - Ensure that the user account has the necessary permissions to send and receive emails.
   - Configure the monitoring system with the appropriate credentials and settings to start the monitoring process.

Recommendations

1. **Regular Monitoring:**
   - Implement a monitoring system that sends test messages at regular intervals (e.g., every 5 minutes) to ensure continuous email server operation.
   - Regular monitoring helps detect and resolve issues quickly, minimizing downtime and maintaining service reliability.

2. **Multiple Alert Channels:**

- Set up multiple alert channels (email, text message, phone call) to ensure that you are promptly notified of any issues.
- Consider the urgency and criticality of your email communications when configuring alert preferences.

3. **User Account Security:**
   - Ensure the user account used for monitoring has a strong password and is secured against unauthorized access.
   - Regularly review and update the account's security settings to maintain a high level of protection.

Conclusion

Monitoring your email server using automated systems ensures that any issues are quickly identified and resolved. One Avenue offers both in-house and third-party monitoring services, providing comprehensive solutions to maintain the reliability of your email system.

By following these recommendations, you can ensure that your email server operates smoothly and efficiently, providing uninterrupted communication for your organization.

Monitoring The Server Messages

Monitoring server messages is an essential task to ensure that your BlueOnyx server operates correctly and efficiently. This includes keeping an eye on messages sent by the server and monitoring the postmaster email account. These messages provide critical information about server updates, performance, and potential issues that may need attention.

Importance of Monitoring Server Messages

1. **Server Operational Messages:**
   - The server will occasionally send out messages that should be monitored to ensure it is operating correctly.
   - These messages include notifications about system updates, performance alerts, and potential issues.

2. **Postmaster Email:**
   - The postmaster email account receives important messages related to the operation of your mail server.
   - Postmaster messages include delivery status notifications, bounce messages, and other email-related alerts.

3. **Update Notifications:**
   - Notifications about available updates are sent to the postmaster email address.
   - These notifications alert the operator to perform necessary updates and reboots to keep the server secure and up-to-date.

Accessing Admin Email

1. **Admin Account:**
   - The admin account can be used with most email clients to monitor these messages.
   - This allows for convenient access to important server notifications and alerts.

2. **Email Forwarding:**

- Admin email can also be forwarded to another address for easier monitoring.

Setting Up Email Forwarding

1. **Access Personal Profile:**
   - Go to the main menu in the BlueOnyx admin interface.
   - Select “Personal Profile” from the menu options.

2. **Enable Email Forwarding:**
   - Click on the “eMail” tab within your personal profile settings.
   - Enable “Email Forwarding” by checking the appropriate box.
   - Set an address that will receive all emails from the server, regardless of their spam status. This ensures that no important messages are missed.

3. **Optional Local Copy:**
   - If desired, you can choose to keep a local copy of the forwarded emails on the server. This can be useful for maintaining a record of all server messages.

Example Configuration

- Forwarding Address: Enter the email address where you want to receive all server messages.
- Keep Local Copy: Enable this option if you want to retain a copy of the emails on the server.

Conclusion

By monitoring the server messages and the postmaster email account, you ensure that your BlueOnyx server is operating correctly and efficiently. Configuring email forwarding helps you stay informed about important updates and alerts, allowing for timely action when necessary. These steps are crucial for maintaining the security and reliability of your server.

Maintaining an Abuse Email Address

Maintaining the email address `abuse@example.com` is a crucial aspect of managing your DNS and mail server using BlueOnyx. This address is not only a best practice but also a requirement under various Internet RFCs (Request for Comments), which are formal documents that define the standards and protocols for the internet.

Importance of an Abuse Email Address

1. **RFC Compliance:**
   - The Internet Engineering Task Force (IETF) publishes RFCs that outline standards for internet operations, including the requirement to maintain an abuse email address.
   - RFC 2142 specifically mandates the existence of `abuse@domain` addresses to handle reports of abuse and other issues related to the domain.

2. **Handling Abuse Messages:**
   - Abuse messages can cover a wide range of issues, including reports of spam, phishing, network abuse, and security vulnerabilities.
   - These messages may come from other mail servers, internet users, security organizations, and automated systems.

Adding an Abuse Email Alias

1. 1. **Setting Up the Alias:**
   - In BlueOnyx, you can set up an alias for the user who will handle the abuse messages.
   - This alias ensures that all emails sent to `abuse@example.com` are forwarded to the appropriate individual or team for action.

2. **Steps to Add the Alias:**
   - Login to BlueOnyx: Open a web browser, navigate to the main IP address of your BlueOnyx server, and log in with your admin credentials.

- Navigate to Site Management: Click on “Site Management” in the main menu and select the domain you wish to manage.
- Modify the Domain: Click on the settings “pencil icon” to modify the domain settings.
- Add Email Alias: In the email settings, add an alias for `abuse@example.com` to the user or group responsible for handling abuse messages.
- Save Changes: Ensure to save the changes to apply the new alias.

Examples of Abuse Messages

1. **Spam Reports:**
   - Messages reporting unsolicited bulk emails originating from your domain.
   - Example: “Your domain is sending spam emails. Please investigate.”

2. **Phishing Alerts:**
   - Reports of phishing emails claiming to be from your domain.
   - Example: “We received a phishing email from your domain. Please address this issue immediately.”

3. **Network Abuse:**
   - Reports of abusive activities such as hacking attempts, DDoS attacks, or other malicious behaviors.
   - Example: “Your IP address is involved in a DDoS attack. Please take action to stop this abuse.”

4. **Security Vulnerabilities:**
   - Notifications about potential security issues or vulnerabilities in your systems.
   - Example: “We have identified a security vulnerability in your server. Please patch it immediately.”

Importance of Maintaining the Abuse Address

1. **Prompt Response:**

- It is very important to maintain a working abuse address to respond promptly to any reports of abuse or security issues.
- Failing to respond to abuse reports can result in your domain being blacklisted or other reputational damage.

2. **Legal and Regulatory Compliance:**
   - Many jurisdictions require businesses to maintain a mechanism for reporting and handling abuse, and failing to do so can have legal repercussions.

3. **Protecting Your Domain and Users:**
   - Addressing abuse reports helps protect your domain from being used for malicious activities, safeguarding your users and maintaining trust in your services.

Conclusion

Maintaining the email address `abuse@example.com` is a vital aspect of managing your DNS and mail server in BlueOnyx. It ensures compliance with internet standards, facilitates the handling of abuse reports, and helps protect your domain's reputation.

By setting up an alias for this address and actively monitoring it, you can effectively manage abuse reports and maintain a secure and trusted email service.

Understanding Updates and Reboots

Keeping your BlueOnyx server up-to-date is essential for maintaining security, performance, and functionality. This involves understanding how updates are managed and when reboots are necessary.

Managing System Updates

1. **Software Update Settings:**
   - The BlueOnyx system will perform updates based on the configuration set under “Software Updates” and then “Settings” in the admin interface.
   - These settings control how and when updates are applied to the system, ensuring that your server remains secure and up-to-date.

2. **Linux Kernel:**
   - The Linux kernel is the core component of the Linux operating system, responsible for managing hardware resources and providing essential services to applications.
   - It acts as a bridge between software applications and the physical hardware of the computer, managing tasks such as memory management, process scheduling, and device communication.

3. **Kernel Updates and Reboots:**
   - When a new kernel is installed during an update, the system must be rebooted to start using the new kernel.
   - Unlike regular application updates, kernel updates require a reboot to take effect because the kernel is the central part of the operating system that runs continuously.

4. **Automatic Reboots:**
   - The system does not automatically reboot for kernel updates to avoid interrupting services during work hours.
   - This approach helps minimize potential downtime and ensures that the reboot can be scheduled at a convenient time.
5. **Application Updates and Reboots:**

- The BlueOnyx system updates a large variety of applications, many of which may need a server reboot to fully apply the updates.
- These updates ensure that the software running on your server is secure and up-to-date but also means that periodic reboots are necessary.

Checking and Installing Updates via Command Line

- Updates can also be checked and installed via the command line using a shell session.
- To update your system, you can use the following command:
  sudo yum update -y
- This command will check for available updates and install them. The `-y` option automatically answers "yes" to any prompts, allowing the update process to proceed without manual intervention.

Scheduling Reboots and Reducing Downtime:

- The update system is designed to reduce potential downtime during work hours by not automatically rebooting after kernel updates.
- It is recommended to schedule reboots during off-peak hours to minimize disruption to services and users.

Conclusion

Maintaining your BlueOnyx server involves understanding the update process and the necessity of reboots. Regular updates keep your server secure and functional, while scheduled reboots ensure that new kernels and critical updates are applied without causing significant downtime.

By managing updates through both the admin interface and the command line, you can ensure your server remains reliable and up-to-date.

Using BlueOnyx for Secure Email Addresses

Setting up a DNS and mail server using BlueOnyx offers flexibility in handling email for specific subdomains, ensuring secure and specialized email addresses. Here's how you can configure your BlueOnyx server to process mail for select subdomains and manage email relays.

Configuring the Server for Specific Subdomains

1. **Selective Mail Processing:**
   - The server does not have to process all the mail for the domain `example.com`. Instead, it can be configured to process mail for specific subdomains such as `mail.example.com`, `secure.example.com`, `peepo.example.com`, or any other subdomain (e.g., `whatever.example.com`).
   - This setup allows you to create and manage email addresses like `user@secure.example.com` or `alias@secure.example.com`.

2. **Using MX Records:**
   - Email is directed to the server using MX (Mail Exchanger) records for the specified hostname that lead back to the server.
   - MX records define the mail servers responsible for receiving email on behalf of a domain or subdomain. They are prioritized using numerical values where lower values have higher priority.

3. **Setting Up MX Records for Email Relays:**
   - When using email relays, you need to add MX records for the relevant subdomains.
   - Here's an example configuration using priority values 10, 30, and 50 for three servers:
     - Primary mail server: Priority 10
     - Secondary relay server: Priority 30
     - Tertiary relay server (if applicable): Priority 50

- Configure the MX record for the main server with a priority of 10 and the new relay server with a priority of 30. This setup ensures that the primary server is used first, and the relay server is used as a backup.

4. **Example MX Record Configuration:**
   - For the main mail server:
     - secure.example.com. IN MX 10 mail.example.com.
   - For the relay server:
     - secure.example.com. IN MX 30 relay.example.com.
     - If you set an MX record priority to 0, email will only go to that server.

Practical Steps

1. **Login to DNS Management:**
   - Login to your DNS management console where your domain's DNS records are hosted.

2. **Add MX Records:**
   - Add an MX record for the primary server with priority 10.
   - Add an MX record for the secondary server with priority 30.

3. **Verify MX Records:**
   - Ensure that the records are correctly added and reflect the intended mail flow.

Conclusion

Using BlueOnyx for secure email addresses provides the flexibility to manage email for specific subdomains, enhancing the security and organization of your email system. By configuring MX records appropriately and using email relays, you can ensure that email is directed to the correct servers, providing a reliable and secure email infrastructure.

Setting Data Retention Rules

Establishing data retention rules is essential for maintaining compliance with legal, regulatory, and security requirements. BlueOnyx provides flexible options for managing data retention, including log files, reports, and email data. Here's how you can set up and manage data retention rules.

Accessing Data Retention Settings

1. Navigate to Data Retention Settings:
   - Log in to the BlueOnyx admin interface.
   - Go to "Server Management" in the main menu.
   - Select "System Settings" and then "Data Retention."

Configuring Log Retention Times and Data Purge

1. **Log Retention Times:**
   - In the "Data Retention" settings, you can configure how long various types of logs are retained on the server.
   - These settings may be required depending on the server's location, legal requirements, and organizational policies.

2. **European Data Retention Requirements:**
   - In Europe, regulations may require maintaining long-term server log files for compliance purposes.
   - Understanding these requirements is crucial for ensuring that your data retention policies align with legal mandates.

Setting Vsite Usage Information Retention

1. **Vsite Usage Information Retention:**
   - This setting allows you to define the length of time to keep server and "virtual host" log files.
   - Adjusting these settings ensures that you retain the necessary information while complying with data retention policies.

2. **Server Logfile Retention:**
   - This section is for system log files, including login history.
   - Keeping a detailed login history may be important for security audits and forensic analysis.

Managing Vsite Usage Information

1. **Impact on Virtual Hosts:**
   - The “Vsite Usage Information” setting will affect all “virtual hosts.”
   - You can set the retention period as desired or as needed for legal or security compliance.
   - Enabling the purge option for site logs will delete the logs after the specified retention period. Enable the switch and click “Save” to apply this setting.

Purging Website Traffic Reports

1. **Purge Webalizer Reports:**
   - Webalizer generates website traffic reports that can accumulate over time.
   - Enable the “Purge Webalizer” switch and click “Save” to remove these reports after a specified period.

Configuring SendmailAnalyzer Data

1. **SendmailAnalyzer Data Expiry:**
   - SendmailAnalyzer generates email reports that can be configured for data retention.
   - Enable the option to “Anonymize data” in the reports by checking the corresponding box and clicking “Save.”
   - This setting helps in protecting sensitive email data while still retaining useful reporting information.

2. **Purge SendmailAnalyzer Data:**

- To remove all data from SendmailAnalyzer, enable the “Purge SendmailAnalyzer” switch and click “Save.”
- This action clears out all the stored email report data.

Practical Steps

1. **Log into the Admin Interface:**
   - Ensure you are logged into the BlueOnyx admin interface to access the settings.

2. **Adjust Settings as Required:**
   - Navigate through the different sections under “Data Retention” to configure each setting according to your needs and compliance requirements.

3. **Save Changes:**
   - Always click “Save” after making changes to ensure that your settings are applied.

Conclusion

By configuring data retention rules in BlueOnyx, you can manage log files, reports, and email data to comply with legal, regulatory, and security requirements. Proper data retention policies help maintain the integrity and security of your system while ensuring compliance with relevant laws and regulations.

Login Manager and Security Functions

In the context of setting up a BlueOnyx server, it is essential to understand the "Login Manager" and related security functions. These tools help ensure the security of your server by monitoring failed logins and managing access control. Here's how you can configure and utilize these security features to protect your BlueOnyx server.

By following these steps, you will be able to configure and utilize the "Login Manager" and related security functions in BlueOnyx effectively. Monitoring failed logins, whitelisting IPs, adjusting PHP settings, and keeping an eye on system processes, logins, and logs are crucial for maintaining a secure server environment.

Monitoring Failed Logins

By default, BlueOnyx monitors for failed login attempts to prevent unauthorized access. This feature helps in identifying potential security threats and ensures that any suspicious activity is promptly addressed.

Viewing and Resetting Failed Logins

1. Login as Admin:
- Open a web browser and navigate to the main IP address of your BlueOnyx server.
- Login using the username "admin" and the password you created during the installation process.

2. Access Security Settings:
- Click on "Security" in the main menu.

3. View Failed Logins:
- Under the "Failed Logins" section, you can view the current list of failed login attempts.
- If a user becomes blocked due to multiple failed password attempts, you can reset the failed login counter to unblock the user.

Configuring the Login Manager

The "Login Manager" in BlueOnyx allows you to manage IP whitelisting and set rules for blocking IPs after a certain number of failed login attempts.

1. Whitelisting IPs:
- Within the “Security” section, navigate to “Login Manager.”
- You can add specific IP addresses to the whitelist to ensure they are not blocked by the failed login rules.

2. Setting Host Rules:
- The host rule dropdown allows you to configure how long an IP will be blocked based on the number of failed attempts within a single hour.
- You can also disable the “Login Manager” completely if desired, though this is generally not recommended for security reasons.

Adjusting PHP Settings

1. Access PHP Settings:
- Under the “Security” menu, you can adjust the server’s default PHP settings to enhance security.
- These settings allow you to configure various PHP options to ensure the server operates securely and efficiently.

Monitoring System Processes, Logins, and Logs

1. Viewing System Processes:
- In the “Security” section, click on “Processes” to view the current system processes.
- This allows you to monitor the running processes and identify any unusual activity.

2. Monitoring Logins:
- Click on “Logins” under the “Security” menu to monitor all login attempts.
- This feature helps track successful and failed login attempts, providing insight into who is accessing your server.

3. Checking System Logs:
- Under the “Security” menu, click on “Logfiles” to view the system logs.
- Regularly monitoring these logs helps in identifying and troubleshooting any potential security issues.

These measures help protect your server from unauthorized access and ensure that any security threats are promptly addressed.

Using a Secure Address and Calendar System

In the context of setting up a secure address and calendar system using BlueOnyx, it is important to understand the functionalities provided by CalDAV and CardDAV. BlueOnyx uses Radicale by default to manage these services. While their use is optional, they allow users to create local and secure calendars and contact lists compatible with popular applications and operating systems, sometimes requiring extensions.

What are CalDAV and CardDAV?

CalDAV (Calendar Distributed Authoring and Versioning) and CardDAV (vCard Extensions to Web Distributed Authoring and Versioning) are protocols that allow users to access and manage calendar and contact data on a server. These protocols ensure that data can be synchronized across multiple devices and applications, providing a seamless experience for managing appointments and contacts.

How BlueOnyx Implements CalDAV/CardDAV

BlueOnyx utilizes Radicale, a simple and efficient CalDAV and CardDAV server, to handle these protocols. Radicale is integrated into BlueOnyx to provide a secure and local solution for managing calendars and contacts.

Components of the System:

- **The Daemon:** This is the server component that manages the CalDAV and CardDAV services. It is controlled via the server settings section and requires configuration by the server admin.
- **Per User Interface:** Located under “CalDAV/CardDAV” in each user’s profile, this interface allows individual users to manage their address books and calendars.

Setting Up CalDAV/CardDAV in BlueOnyx

Server Configuration

1. Login as Admin:

- Open a web browser and navigate to the main IP address of your BlueOnyx server.
- Login using the username “admin” and the password you created during the installation process.

2. Access Network Settings:
- Click on “Network Settings” in the main menu.

3. Enable Radicale:
- Click on “CalDAV/CardDAV” in the settings menu.
- Enable Radicale and use the default settings provided.
- Configure any additional settings to meet your specific requirements.
- Click “Save” to apply the settings.

User Configuration

1. Personal Profile Settings:
- After logging in as admin, navigate to “Personal Profile” from the main menu.
- Click on “CalDAV/CardDAV” to access the user-specific settings.

2. Creating Address Books and Calendars:
- Click on “Add” to create new address books and calendars.
- You can manage these entries by adding, editing, or deleting as needed.

3. Backup and Restore:
- It is recommended to regularly create backups of your address books and calendars.
- You can perform backups and restores directly from the CalDAV/CardDAV interface.

4. Connecting to Radicale GUI:
- Users can connect and login to the Radicale GUI for more advanced management options.
- Copy the URL of the address document or calendar for use in client applications.

Conclusion

By following these steps, you will have successfully set up a secure and efficient address and calendar system using BlueOnyx and Radicale. This setup allows you to maintain local control over your data, ensuring security and privacy. Regular backups are essential; ensure they are stored in a secure location. This comprehensive approach will enhance the management of your schedules and contacts while maintaining the highest security standards.

Installing and Configuring SpamAssassin

SpamAssassin is an open-source spam filtering tool that can detect and delete spam messages, significantly reducing the amount of unsolicited email in your inbox. Here's a detailed guide on what SpamAssassin is, how to install and configure it on a RedHat 9 clone system, and how to set up various procmail scripts to handle spam effectively.

What is SpamAssassin?

SpamAssassin is a powerful spam filter that uses a variety of tests to identify and block spam emails. It analyzes emails for characteristics typical of spam and assigns a score to each message. Messages that exceed a certain score threshold are marked or discarded as spam.

Control Panel Package for BlueOnyx

A full control panel package for managing SpamAssassin is available at [BlueOnyx.it](http://blueonyx.it). This package provides an easy-to-use interface for configuring and managing SpamAssassin on your server.

Basic Installation of SpamAssassin

- The basic installation of SpamAssassin on BlueOnyx uses procmail with updates provided by a cron job.

Installing SpamAssassin as a Daemon

1. **Install SpamAssassin:**
   - To install SpamAssassin and its dependencies, run the following command:
     yum install spamassassin

2. **Install Additional Perl Modules:**
   - SpamAssassin requires several Perl modules to run additional tests. Install these modules using the following command if desired:


```
yum install perl-Archive-Zip perl-IO-String.noarch perl-Net-Patricia
```

Configuring SpamAssassin

Configuration Files:

- The main configuration files for SpamAssassin are located in `/etc/mail/spamassassin`.
- You can customize SpamAssassin's behavior by editing these configuration files using a text editor like `nano`. For example:

```
nano /etc/mail/spamassassin/local.cf
```

What is Procmail?

Procmail is a mail processing utility used to filter, sort, and process incoming mail. It uses scripts called procmail recipes, which define how emails should be handled.

Sample Procmail Scripts

1. Delete Messages with Spam Score Above 3.5:

```
:0:
* ^X-Spam-Level: \*\*\*\*\*\*\*
/dev/null
```

2. Tag Messages with Spam Score Above 3.5:

```
:0
* ^X-Spam-Level: \*\*\*\*\*\*\*
{
  :0 fhw
  | /usr/bin/spamc -e 'formail -i "X-Spam-Status: Yes" -i "X-Spam-Flag: YES"'
}
```

3. Send All Spam to a Folder:

```
:0:
* ^X-Spam-Level: \*\*\*\*\*\*\*
```


/var/mail/spam-folder or “spam” for the users directory.

4. Send All Spam Messages to junk@example.com:

```
:0:
* ^X-Spam-Level: \*\*\*\*\*\*\*
! junk@example.com
```

Note: Ensure that the `junk@example.com` account or alias is created.

5. Check SpamAssassin score and tag as [SPAM] if score is above 2.5

```
:0
* ^X-Spam-Level: \*\*\*\*\*
{
    :0
    * ^Subject:\/.*
    {
        SUBJECT=$MATCH
        :0 fhw
        | formail -I "Subject: [SPAM] $SUBJECT"
    }
}

# Deliver to default mailbox
:0
$DEFAULT
```

6. CC another eMail address

```
# Email address to CC all mail to
CC_ADDRESS="cc@example.com"

# Rule to CC all incoming mail
:0 c
! $CC_ADDRESS

# Deliver the original mail to the default mailbox
:0
```


File Permissions for Procmail Configuration Files

Proper file permissions for procmail configuration files are crucial to ensure the correct and secure functioning of your mail processing setup. The main system-wide procmail configuration file is located at `/etc/procmailrc`. This file should be owned by the root user to prevent unauthorized modifications that could disrupt mail processing or compromise system security. Typically, the permissions for this file should be set to `644` (read and write for the owner, and read-only for others), ensuring that only the root user can modify it, while other users can read it as needed.

For user-specific procmail configuration files, which are located in each user's home directory as `.procmailrc`, appropriate permissions are equally important. These files should be owned by the respective user and have permissions set to `600` (read and write for the owner, and no permissions for others). This ensures that only the user can read and modify their procmail configuration, preventing other users from accessing or altering their mail processing rules. To set these permissions, you can use the following commands:

For `/etc/procmailrc`:
sudo chown root:root /etc/procmailrc
sudo chmod 644 /etc/procmailrc

For `.procmailrc` in a user's home directory:
chown username:username /home/username/.procmailrc
chmod 600 /home/username/.procmailrc

Replace `username` with the actual username. Ensuring these permissions are correctly set helps maintain the integrity and security of your mail processing environment.

Enabling SpamAssassin at Boot

- To ensure that SpamAssassin starts automatically at boot, use the following command:
    systemctl enable spamassassin

Updating SpamAssassin Rules

To activate `/usr/share/spamassassin/sa-update.cron` for daily updates, follow these steps:

1. **Create a Symlink in the cron.daily Directory**

To ensure that SpamAssassin updates run daily, create a symbolic link in the `/etc/cron.daily` directory pointing to `/usr/share/spamassassin/sa-update.cron`. Use the following command:

ln -s /usr/share/spamassassin/sa-update.cron /etc/cron.daily/sa-update

1. **Ensure Execute Permissions**

Make sure the `sa-update.cron` script has execute permissions. Set the appropriate permissions with the following command:

chmod +x /usr/share/spamassassin/sa-update.cron

By creating a symlink in `/etc/cron.daily` and ensuring the `sa-update.cron` script has execute permissions, the system will automatically run SpamAssassin updates daily.

This setup keeps your spam rules current and enhances the effectiveness of your spam filtering.

Conclusion

By configuring SpamAssassin on your BlueOnyx server, you can effectively manage and filter spam emails, ensuring that your inbox remains clean and secure. Use the provided instructions and sample procmail scripts to set up and customize SpamAssassin to meet your specific needs.

Integrating GeoLite2 Databases with SpamAssassin

Introduction

SpamAssassin is a powerful spam filtering tool that can utilize geographical data to enhance its filtering capabilities. By integrating GeoLite2 databases, you can enable SpamAssassin to make better decisions based on the geographical origin of emails.

1. **Install GeoLite2 Databases**

   - To begin, install the GeoLite2 databases. These databases provide the geographical information that SpamAssassin will use.

     yum install geolite2-city geolite2-country

This command installs the `geolite2-city` and `geolite2-country` packages, which include the GeoLite2 databases.

2. **Configure SpamAssassin to Use GeoLite2 Databases**

   - Next, configure SpamAssassin to recognize and use the GeoLite2 databases. This involves modifying the SpamAssassin configuration files.

   A. **Locate the GeoLite2 Database Files:**

      - After installation, the database files are typically located in the `/usr/share/GeoIP/` directory. Verify the exact location by listing the contents of the directory.

      ls /usr/share/GeoIP/

   B. **Edit the `init.pre` File:**

      - The `init.pre` file is where you will specify the paths to the GeoLite2 databases. This file is usually found in the `/etc/mail/spamassassin/` directory.
      - nano /etc/mail/spamassassin/init.pre

C. **Add or Uncomment the Required Lines:**

- In the `init.pre` file, ensure the following lines are added or uncommented to configure SpamAssassin to use the GeoLite2 databases:

```
loadplugin Mail::SpamAssassin::Plugin::RelayCountry
loadplugin Mail::SpamAssassin::Plugin::URILocalBL

# Path to the GeoLite2 databases
geodb_path /usr/share/GeoIP/geolite2-City.mmdb
geodb_path /usr/share/GeoIP/geolite2-Country.mmdb
```

D. **Save and Exit:**

- Save the changes and exit the editor.

3. **Restart SpamAssassin**

- After configuring the paths to the GeoLite2 databases, restart the SpamAssassin service to apply the new settings.

```
systemctl restart spamassassin
```

4. **Verify the Configuration**

Finally, verify that SpamAssassin correctly loads the GeoLite2 databases by running the `spamassassin -D --lint` command. This command will perform a detailed lint check and output debug information.

```
spamassassin -D --lint
```

Ensure that the output does not show any errors related to the GeoLite2 databases. If the modules are correctly installed and configured, you should not see any "optional module not installed" messages.

Conclusion

By following these steps, you can successfully integrate GeoLite2 databases with SpamAssassin. This enhancement allows SpamAssassin to leverage geographical data, improving its ability to detect and filter spam based on the origin of the emails

Editing the SpamAssassin Configuration in `local.cf`

To customize how SpamAssassin handles spam emails and forwards error messages, you need to edit the `local.cf` configuration file. Here's a detailed explanation of key settings you can configure to optimize spam filtering and handling.

Accessing and Editing the Configuration File

1. **Open the Configuration File:**
   - Use a text editor like `nano` to open the `local.cf` file. This file contains the main configuration settings for SpamAssassin.

     nano /etc/mail/spamassassin/local.cf

Key Configuration Options

Below are some critical settings you can add or modify in the `local.cf` file to enhance SpamAssassin's functionality:

1. **required_hits 5:**
   - Purpose: This setting specifies the number of hits (or points) an email must accumulate before it is considered spam.
   - Usage: The default value is usually higher, but setting it to 5 makes the spam filter more aggressive.

2. **report_safe 0:**
   - Purpose: Disables the automatic safe-reporting feature. When set to `0`, SpamAssassin will not encapsulate spam messages in an attachment. Instead, it will modify the original message directly.
   - Benefits: Easier management and forwarding of spam messages since the original email structure is maintained.

3. **rewrite_header Subject [SPAM]:**

- Purpose: This setting rewrites the subject line of emails identified as spam to include a specified tag, such as `[SPAM]`.
- Benefits: Helps users easily identify and filter spam messages in their inbox.

4. **envelope_sender_header X-MailFrom:**
   - Purpose: Specifies the header that SpamAssassin will use to determine the envelope sender. The `X-MailFrom` header is often used to identify the sender's address.
   - Benefits: Ensures accurate identification of the sender, which can be useful for filtering and reporting.

Example Configuration

Here's an example of how your `local.cf` file might look after making these adjustments:

```
# Set the number of hits required before an email is considered spam
required_hits 5

# Disable the automatic safe-reporting feature
report_safe 0

# Rewrite the email subject to indicate it is spam
rewrite_header Subject [SPAM]

# Specify the header to determine the envelope sender
envelope_sender_header X-MailFrom
```

Applying Changes

5. **Save and Close:**
   - After making your changes in `nano`, save the file by pressing `Ctrl+O`, then press `Enter` to confirm. Exit the editor by pressing `Ctrl+X`.

6. **Restart SpamAssassin:**

- For the changes to take effect, restart the SpamAssassin service. On most systems, you can do this with the following command:

  systemctl restart spamassassin

Understanding the `/etc/mail/spamassassin` Directory

In addition to `local.cf`, the directory includes several pre-configuration files like `init.pre`, `v310.pre`, `v320.pre`, and others, which load specific plugins and features essential for SpamAssassin's operation. These files are crucial for enabling advanced functionalities such as Bayesian filtering, DKIM verification, and SPF checks. By editing these pre-configuration files, administrators can activate or deactivate particular modules, tailoring the spam filtering capabilities to their specific requirements. For example, uncommenting lines in `v320.pre` to load the Bayesian classifier or in `v330.pre` for DKIM verification enhances the accuracy and effectiveness of spam detection.

Other notable files include `sa-update-keys`, `spamassassin-default.rc`, and various helper scripts like `spamassassin-helper.sh`. The `sa-update-keys` file is used to verify the authenticity of rule updates received via `sa-update`, ensuring that only legitimate updates are applied. The `spamassassin-default.rc` file contains the default settings, providing a baseline configuration that can be overridden by `local.cf`. Scripts such as `spamassassin-helper.sh` automate common administrative tasks, making it easier to manage and maintain SpamAssassin. By leveraging these configuration files and scripts, administrators can ensure their spam filtering setup is robust, efficient, and tailored to their organization's specific needs.

Conclusion

By customizing the `local.cf` file, you can fine-tune SpamAssassin’s behavior to better meet your email filtering needs. Adjusting the number of hits required to classify spam, modifying the subject line of spam emails, disabling safe-reporting, and specifying the envelope sender header are all effective ways to enhance the handling of spam on your mail server.

Antivirus and Spam GUI in the BlueOnyx Store

When setting up a BlueOnyx server, comprehensive email security measures, including antivirus and spam protection, are crucial. While this guide provides instructions for basic spam detection using SpamAssassin, it does not include antivirus protection. Antivirus software is not part of the upstream OS and requires constant updates to remain effective against new threats.

Limitations of Basic Spam Detection

Basic spam detection using SpamAssassin provides foundational protection against unwanted emails. However, it lacks the robust features and flexibility of a full antivirus and spam package. Basic setups may not offer advanced filtering capabilities and do not include antivirus scanning, which is crucial for protecting against email-borne malware and viruses.

Comprehensive Antivirus and Spam Package

To address these limitations, BlueOnyx offers a full antivirus and spam package available in the BlueOnyx store. This package provides comprehensive email security with professional support to ensure optimal performance and protection.

Features of the Full Package

Antivirus Protection:

- The package includes a full antivirus solution that integrates seamlessly with your BlueOnyx server. It scans incoming and outgoing emails for viruses, malware, and other malicious content, adding an essential layer of security.

Advanced Spam Filtering:

- In addition to basic spam detection, the package offers advanced spam filtering features. This includes customizable rules, Bayesian filtering, and real-time blackhole lists (RBLs) to enhance spam detection accuracy.

Graphical User Interface (GUI):

- The full antivirus and spam package includes a comprehensive GUI. This interface allows both administrators and users to control various settings, making it easy to configure and manage email security policies.

Administrative Controls

Administrators can use the GUI to:

- Configure antivirus and spam filtering settings.
- Define global policies for handling spam and infected emails.
- Monitor email traffic and view detailed logs and reports.
- Set up automatic updates to ensure the antivirus definitions are always current.

User Controls

End-users can also benefit from the GUI by:

- Adjusting personal spam filtering preferences.
- Whitelisting or blacklisting specific email addresses or domains.
- Reviewing quarantined emails to recover legitimate messages that may have been flagged as spam.

Professional Support

The package includes access to professional support, ensuring that you have expert assistance available when needed. This support can help with initial setup, troubleshooting, and ongoing maintenance, providing peace of mind that your email security is in good hands.

Conclusion

While basic spam detection using SpamAssassin offers a starting point for email security, the comprehensive antivirus and spam package available in the BlueOnyx store provides a more robust solution.

With full antivirus protection, advanced spam filtering, a user-friendly GUI, and professional support, this package ensures that your BlueOnyx server is well-equipped to handle the evolving landscape of email threats.

This enhanced security framework not only protects your server but also helps maintain the integrity and confidentiality of your email communications.

Installing Web Applications and Creating Websites

BlueOnyx is a versatile web server platform capable of hosting a wide variety of web applications. These applications can range from content management systems like WordPress and e-commerce platforms like Magento to web frameworks and templates like Bootstrap. Here's a detailed guide on how to install and manage web applications on BlueOnyx.

Hosting a large variety of web Applications

Supported Applications:

- BlueOnyx can host a wide range of web applications, including:
- WordPress: A popular content management system used for creating blogs and websites.
- Magento: A robust e-commerce platform for online stores.
- Bootstrap Templates: Front-end templates for creating responsive websites.
- Other web applications and frameworks can also be hosted on BlueOnyx, making it a flexible solution for various web development needs.

Installation and Downloading Instructions

Source of Applications:

- Always download web applications from their official developer sites to ensure you receive the latest, most secure versions.
- Avoid using third-party sites, which may provide outdated or compromised versions of the applications.

File Transfer to the Server

1. **Using FTP:**
   - Most web applications require files to be transferred to the server using FTP (File Transfer Protocol).

- Ensure you have an FTP client installed on your computer, such as FileZilla or WinSCP.

2. **Website Root Folder:**
   - The main website folder or root folder on BlueOnyx is located at:
     /home/sites/www.example.com/www/wwwroot/

   Replace `www.example.com` with your actual domain name.

1. **Removing Default Index File:**
   - The root folder may contain a default `index.html` file, which should be removed before uploading your web application files.
   - You can remove it via FTP or by using an SSH command:

   rm /home/sites/www.example.com/www/wwwroot/index.html

Transferring Files with Siteadmin Privileges

- The files should be transferred by a user with “siteadmin” privileges to ensure proper permissions and access.
- Users with siteadmin privileges have their home directories located at:

/home/sites/www.example.com/home/users/username

Replace `username` with the actual username.

About Connecting via FTP:

- When a user connects via FTP, they may need to navigate to the website folder. Use the following command to change directories:

  cd ../../../wwwroot/web/

- This command navigates to the appropriate web root directory where web application files should be uploaded.

Steps for Installing a Web Application (e.g., WordPress)

1. **Download WordPress:**
   - Visit the official WordPress site and download the latest version.

2. **Upload Files to Server:**
   - Use an FTP client to upload the WordPress files to the root folder:

   /home/sites/www.example.com/www/wwwroot/

3. **Create a Database:**
   - Login to your BlueOnyx control panel.
   - Navigate to “MySQL Management” and create a new database and user for WordPress.

4. **Run the WordPress Installation:**
   - Open a web browser and navigate to your domain (e.g., `http://www.example.com/install`).
   - Follow the WordPress installation wizard, providing the database details created earlier.

Conclusion

BlueOnyx provides a robust and flexible platform for hosting various web applications. By following these detailed instructions, you can effectively set up and manage web applications, ensuring your websites are up-to-date, secure, and efficiently managed.

Always remember to download applications from official sources, manage files using siteadmin privileges, and properly configure your server environment to support your web applications.

Advanced Options in BlueOnyx

When setting up a DNS, mail server, or website using BlueOnyx, it's important to understand that the platform offers a vast array of advanced options and configurations. While this guide covers the basic setup, BlueOnyx's capabilities extend far beyond these fundamentals. Here's an overview of the more advanced aspects and considerations to keep in mind.

1. **Extensive Configuration Possibilities:**
   - BlueOnyx is built on standard Linux distributions, which inherently provide hundreds of built-in options and tools for various tasks.
   - These advanced options can include custom scripting, detailed security configurations, specialized network settings, and more.

2. **Potential Conflicts with the Control Panel:**
   - While BlueOnyx offers a user-friendly control panel for managing your server, some advanced configurations performed directly via the command line or other methods may conflict with the control panel settings.
   - It's crucial to be aware of these potential conflicts and understand how to manage them if you choose to explore advanced configurations.

BlueOnyx as a Long-Term Production Server

1. **Designed for Stability and Reliability:**
   - BlueOnyx is specifically designed to be a long-term production web services server, emphasizing stability, reliability, and security.
   - It is not intended to serve as a “programmer’s playground” where constant changes and experimental setups are the norm.

2. **Focus on Production Use:**
   - The platform is tailored for environments where consistent performance and uptime are critical, such as business websites, email servers, and other professional services.

- This focus ensures that your services remain robust and dependable over time.

Exploring Advanced Options Safely

1. **Documentation and Support:**
   - Before making any advanced changes, consult the comprehensive documentation available for BlueOnyx and the underlying Linux distribution.
   - Consider reaching out for BlueOnyx support or engaging with community forums for guidance and best practices.

2. **Testing and Validation:**
   - If you decide to implement advanced configurations, always test changes in a controlled environment before applying them to your production server.
   - Validate that these changes do not negatively impact the stability or performance of your server.

3. **Backup and Recovery:**
   - Ensure you have a reliable backup and recovery strategy in place before making any significant changes.
   - Regularly back up your server configurations and data to quickly restore your system in case of issues.

Conclusion

BlueOnyx offers a powerful and flexible platform for setting up DNS, mail servers, and websites, with a wealth of advanced options available for those who require them. However, it is essential to approach these advanced configurations with caution, understanding the potential for conflicts and the need for stability in a production environment. BlueOnyx is designed to provide long-term, reliable web services rather than serve as a platform for constant experimentation.

Supporting BlueOnyx

BlueOnyx is a robust and versatile platform for setting up DNS and mail servers. However, to ensure its continued development and maintenance, it relies on a network of support and funding. Here's an overview of the support structure for BlueOnyx and how you can contribute to its sustainability.

History of BlueOnyx Support

1. **Private Support Post-Discontinuation:**
   - BlueOnyx originated from a parent product that was eventually discontinued. When this happened, the control panel was made open-source, allowing developers to continue its development.
   - Since then, BlueOnyx has been privately supported by a dedicated team of developers and contributors.

2. **Maintenance of Update Servers:**
   - Maintaining the network of update servers is crucial for providing timely and reliable system updates.
   - System updates ensure that BlueOnyx remains secure, stable, and up-to-date with the latest features and security patches.

Time-Consuming Nature of Support

1. **Effort and Resources:**
   - Supporting BlueOnyx is a time-consuming endeavor that involves constant monitoring, development, and troubleshooting.
   - Developers need to ensure compatibility with various hardware configurations, manage update servers, and respond to user feedback and issues.

2. **Funding Through Donations and Service Packages:**
   - BlueOnyx is completely funded by donations and the sale of additional service packages.

- These contributions are essential for sustaining the project, covering server costs, and compensating the development team's efforts.

Additional Services and Packages

1. **Available Packages:**
   - A variety of additional packages are available in the BlueOnyx online store, enhancing the platform’s functionality and security. These packages include:
   - **ClamAV:** An open-source antivirus engine designed for detecting trojans, viruses, malware, and other malicious threats.
   - SpamAssassin: A powerful spam filter used to identify and block spam emails.
   - **RoundCube:** A web-based IMAP email client that provides a user-friendly interface for managing emails.
   - And Many More: Additional packages that offer extended capabilities, such as enhanced security features, administrative tools, and user interfaces.

2. **Supporting the Project:**
   - By purchasing these packages or making donations, you directly support the ongoing development and maintenance of BlueOnyx.
   - These contributions help ensure that the platform remains viable, secure, and feature-rich for all users.

Conclusion

Supporting BlueOnyx is vital for its continued success and sustainability. Since the discontinuation of its parent product, BlueOnyx has relied on a dedicated network of private support, donations, and the sale of additional service packages. Maintaining the update servers and ensuring system updates is a time-consuming process, but it is essential for keeping the platform secure and up-to-date. By contributing through donations or purchasing additional packages, you help sustain this valuable resource, ensuring its availability and continued development for users worldwide.

One Avenue: BlueOnyx Installation Support

In the realm of professional communications, having a secure, reliable, and efficient email server is crucial. One Avenue offers premium support services tailored to help you set up and maintain a top-notch email server. Whether you want to take full control with the “Do the Hillary” package or prefer a hands-off approach with our “Just Do It” service, One Avenue has you covered.

“Do the Hillary” Email Server Installation

Our “Do the Hillary” service is designed to assist you with the complete remote installation of a dedicated email server. This includes DNS configuration and ensuring your server operates on a reputable IP for optimal performance. Here’s what you get:

- **Comprehensive Installation:** We handle the complete installation of the operating system, specifically tailored to function as a robust email server.
- **Unlimited Support:** Benefit from unlimited hours of direct phone support and unlimited ticket support for one month. Our team is ready to resolve any issues quickly and efficiently.
- **Ongoing Maintenance:** For continuous peace of mind, we offer optional monthly support plans. These plans include ongoing monitoring and maintenance to keep your server secure, reliable, and up-to-date.
- **Ideal for Professionals:** This service is perfect for professionals who require a dependable email communication setup without the technical hassle.

Available Add-Ons

To further enhance your server’s capabilities, consider our additional services:

- **Secondary DNS and Email Relay Service:** Ensure your essential communications and domain accessibility are never compromised. Our globally distributed MX servers provide an always-on, fail-safe email reception system, including support for up to five domain names. This service is available for $19.95 USD monthly.

One Avenue: A Secure Communication Infrastructure for the Modern Age

In today's digital era, where client confidentiality and data security are paramount, legal professionals and other high-stakes industries face a pressing need to modernize their electronic communication systems. One Avenue serves as an industry exemplar, offering a comprehensive suite of services designed to meet these needs with precision and security. While One Avenue provides a ready-made solution, it also serves as an illustrative model that can be adapted or replicated according to specific organizational needs.

The Essence of the One Avenue Model

One Avenue stands as a testament to integrating two vital aspects: connectivity and security. Their framework hinges on a nexus of high-speed internet exchanges and a robust security architecture. This integration embodies the dual goals of streamlining communications while keeping them fortified against external threats. Here’s part of how One Avenue achieves this:

Web Hosting Solutions

One Avenue offers a range of web hosting solutions tailored to different needs:

- **Basic Hosting:** Ideal for small websites and personal projects, providing reliable uptime and essential features.
- **Business Hosting:** Designed for growing businesses, offering enhanced performance, additional resources, and greater support.
- **Professional Hosting:** Suitable for high-traffic sites and complex applications, ensuring maximum uptime and advanced security measures.
- **WordPress Hosting:** Optimized for WordPress, featuring pre-configured settings, automatic updates, and robust security measures to ensure smooth and secure operation of WordPress sites.

eMail Servers and Relays

Reliable email communication is critical for any professional setting. One Avenue provides:

- **eMail Servers:** Fully managed email servers that ensure your communications are secure, confidential, and reliable. Our servers support advanced features like spam filtering, encryption, and data loss prevention.
- **eMail Relays:** Enhance your email deliverability and reliability with our email relay services. These are designed to handle high volumes of email traffic, ensuring your messages reach their intended recipients without delay or loss.

Secondary DNS Servers

To ensure uninterrupted access to your online services, One Avenue offers secondary DNS servers. These servers provide:

- **Redundancy:** By having multiple DNS servers, you mitigate the risk of downtime due to a single point of failure.
- **Failover Capability:** In case your primary DNS server goes down, the secondary DNS server automatically takes over, ensuring continuous access to your websites and email services.
- **Enhanced Security:** Secondary DNS servers add an extra layer of protection against DNS attacks, helping to safeguard your online presence.

Conclusion

One Avenue has charted a course demonstrating how electronic communication infrastructure can be modernized to prioritize confidentiality and security. As an industry leader, One Avenue offers a comprehensive suite of services—web hosting, email servers, email relays, and secondary DNS servers—that together create a robust, secure communication framework.

However, One Avenue is just one example. As the landscape of digital communication and threats evolves, professionals must actively consider, adapt, and implement systems that uphold the highest standards of their profession. Whether choosing to collaborate with existing service providers like One Avenue, building their own infrastructure, or utilizing other available solutions, the goal remains the same: unwavering protection of client data in a digital world.

By choosing One Avenue, you are not only adopting a secure and efficient communication infrastructure but also ensuring that your digital communications are safeguarded by a provider committed to excellence and security.

