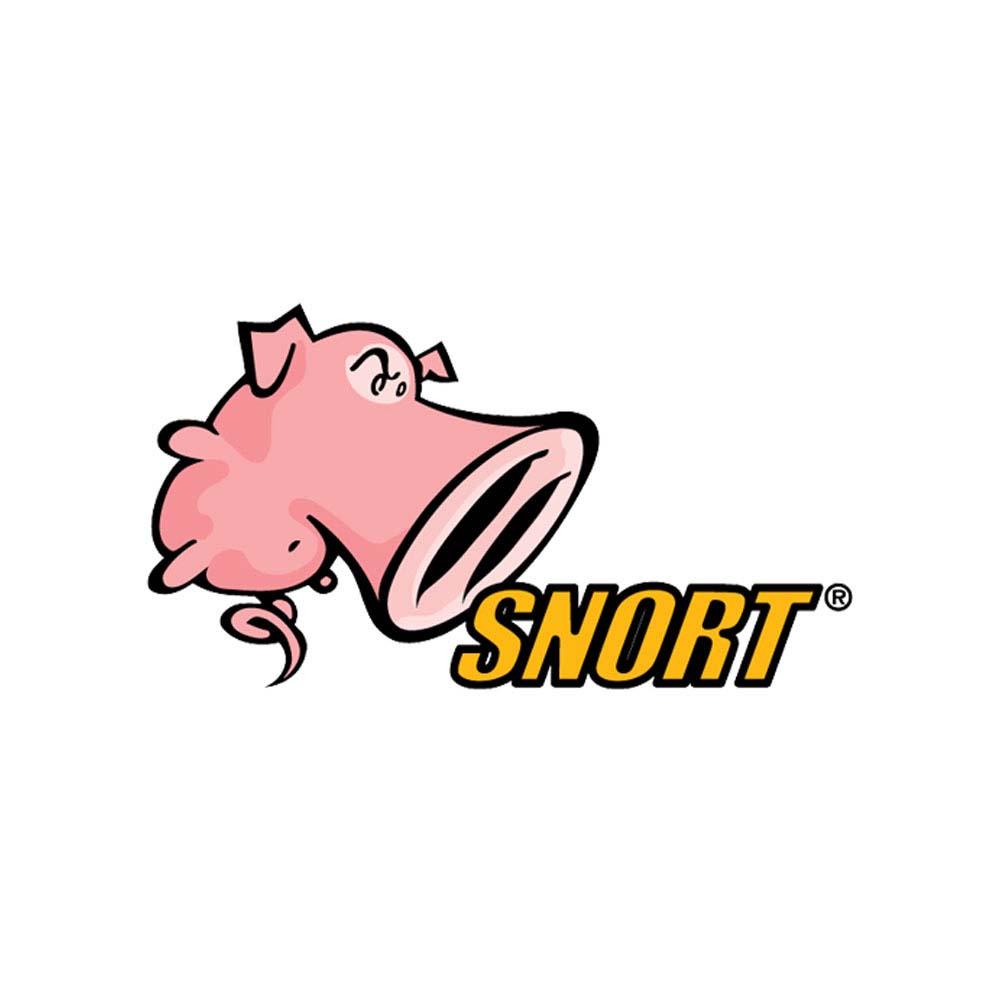
****

**TECHNICAL MANUAL**

IDS/IPS Setup

Windows 2022 AD Server

**Prepared By :** Mark Byrne **Prepared on :** *25/6/23*

**Table of Contents**

[**Introduction 3**](#_3tw1tfp6ilmb)

[Purpose and Scope 3](#_4g922dfjp7g)

[Overview of Snort 3](#_n9693987hin7)

[Key Features 3](#_v8g7ixpwvgmd)

[Prerequisites 3](#_5d1bmywhb43k)

[Document Structure 3](#_tfhqzgf1583a)

[Document Revision History 3](#_h3doh9uof2zt)

[**Installation and Configuration 4**](#_p1jxhvpkrdcx)

[**User Management 10**](#_kykzhxbretpn)

[User roles and permissions 10](#_fwyuvvvm82qa)

[Creating and managing user accounts 10](#_ie6gcaxqrx00)

[Defining and assigning roles and capabilities 10](#_fuu5ft8599n1)

[Authentication options 10](#_hx0qci70v0vo)

[To configure authentication options: 10](#_oyv757288stg)

[**Data Ingestion 11**](#_lhllkn5ix1hl)

[Data Input Options: 11](#_8s78b778kalc)

[Configuring and Managing Data Inputs: 11](#_pgbjir8obqkp)

[Setting Up Sourcetypes and Automatic Field Extraction: 11](#_nah1q9abgn40)

[Managing Data Input Pipelines and Sourcetypes: 11](#_hy63ib11sqaw)

[**Output Analysis 12**](#_z6ms8e4ei5ol)

[Alert File Analysis: 12](#_eeui2lchc0ep)

[Log File Analysis: 12](#_ay2gkfbrx6o7)

[**Data Management 14**](#_1ggo7hdx427e)

[Indexing Configuration 14](#_49a2c0nqlp17)

[Managing Indexes 14](#_60lybkaeeus8)

[Data Lifecycle Management 14](#_cd92pqcxaxgl)

[**Security and Access Control 15**](#_6s7sw1fior01)

[Securing Program Deployments 15](#_1h9ut2jbompi)

[User Authentication and Authorization 15](#_g7ueoqbabnqy)

[Role-Based Access Control (RBAC) and Permissions 15](#_v3qleymymi9c)

[Implementing SSL/TLS Encryption for Data in Transit 15](#_qab6c77hcq9l)

[**Maintenance and Upgrades 16**](#_h95bfxyrn6px)

[Routine Maintenance Tasks 16](#_3yo621spsu13)

[Applying Updates and Patches 16](#_4kbwq7v11id0)

[Backup and Disaster Recovery Procedures 16](#_xzdt0k7ghm6y)

[Version Compatibility Considerations and Upgrade Planning 16](#_wsj85eixdgpx)

[**Resources and References 16**](#_ldyp51g9o88)

[Snort Official Documentation: 16](#_4gewmgj3pq71)

|  |
| --- |
| Introduction |
| Purpose and Scope The purpose of this document is to provide an introduction to Snort, an open-source network intrusion detection and prevention system (NIDS/NIPS). It aims to familiarise users with the features, capabilities, and benefits of Snort in monitoring and analysing network traffic for potential security threats and attacks. Overview of Snort Snort is an open-source network intrusion detection and prevention system (NIDS/NIPS) developed by Sourcefire. It is widely used to monitor and analyze network traffic for potential security threats and attacks. Snort can detect a variety of suspicious activities, such as port scanning, network reconnaissance, and known attack patterns, by examining packet headers and payloads. Key Features  * Network intrusion detection: It analyzes network traffic in real-time to identify potential security threats and attacks. * Network intrusion prevention: Snort can actively block or prevent malicious traffic from reaching its intended destination. * Rule-based detection: It uses a set of pre-defined rules to identify known attack patterns and suspicious activities. * Signature-based detection: Snort compares packet headers and payloads against signatures of known threats to trigger alerts. * Protocol analysis: It supports a wide range of network protocols and can analyze their usage and behavior. * Flexible rule customization: Users can define custom rules to detect specific threats or modify Snort's behavior. * Extensibility: Snort can be extended through the use of plugins, preprocessors, and output modules to enhance its functionality. * Logging and alerting: It can generate detailed logs and alerts when suspicious activities are detected. * Integration capabilities: Snort can be integrated with other security tools and systems for enhanced threat detection and response. * Platform compatibility: It can be deployed on various operating systems, including Windows, Linux, and macOS  Prerequisites The minimum requirements for installing and using Snort on Windows are as follows:   * Operating System: Windows 7, Windows 8, Windows 10, or Windows Server (2008, 2012, 2016, or later versions). * Processor: Intel Pentium 4 processor or equivalent (or higher) with at least 2 GHz clock speed. * RAM: Minimum 1 GB of RAM (2 GB or more is recommended for better performance). * Disk Space: Snort requires approximately 400 MB of disk space for the installation. However, additional space is required for log files, rule sets, and any additional data storage needs. * Network Interface: A supported network interface card (NIC) capable of packet capturing and promiscuous mode operation. It's essential to ensure that the NIC drivers are properly installed and up to date.   Software Dependencies:   * WinPcap or Npcap: Snort relies on a packet capture library for network traffic analysis. WinPcap (Windows Packet Capture) or Npcap (a newer alternative) needs to be installed on the Windows system to capture packets. * Microsoft Visual C++ Redistributable: Depending on the specific version of Snort you are using, you may need to install the Microsoft Visual C++ Redistributable package.  Document StructureDocument Revision History |

Version 1.0 - Mark Byrne - 26/6/2023

|  |
| --- |
| Installation and Configuration |
| * Pre-installation requirements (supported operating systems, hardware, software dependencies) * Installation steps for different platforms (Windows, Linux, macOS) * Configuration options during installation (admin password, ports, etc.) * Post-installation tasks (initial setup wizard, licence installation)   Step One: Download Snort - Visit the official Snort website (www.snort.org) and download the latest Windows version of Snort. Choose the appropriate installer package for your Windows version.    Step two: Install Snort - Run the installer package and follow the on-screen instructions to install Snort on your Windows machine. Choose the desired installation directory and components to install.    Step 2a: Install NpCap - Download and run the installer package and follow the on-screen instructions to install NpCap on your Windows machine. Choose the desired installation directory and components to install.    Step 3: Configure Snort: Snort's configuration is managed through a configuration file called "snort.conf". Locate the "snort.conf" file, which is usually located in the Snort installation directory (e.g., C:\Snort\etc\snort.conf).    Step 4: Customize the configuration: Open the "snort.conf" file in a text editor and customize it according to your needs. Configure parameters such as network interface, preprocessor settings, rule paths, and logging options. You can also enable or disable specific rules or preprocessors based on your requirements.   * Configure rules: Snort uses rules to detect specific threats. You can download rule sets from trusted sources like Snort.org or create custom rules. Update the "snort.conf" file to include the path to your rule files. (See below for more detail)     Step 5: Start Snort - Open a command prompt with administrative privileges and navigate to the Snort installation directory ( C:\Snort\bin). Use the command snort -i <interface> -c <path\_to\_snort.conf> to start Snort, replacing <interface> with the network interface you want Snort to monitor and <path\_to\_snort.conf> with the path to your customized "snort.conf" file.  To enable Network Intrusion Detection System (NIDS) mode the command is::  Snort -i 168.192.0.101-c C:\snort\etc\snort.conf  This will configure Snort to run in its most basic NIDS form, logging packets that trigger rules specified in the snort.conf in plain ASCII to disk using a hierarchical directory structure (See output analysis below for more details)  **Snort Rules Configuration**  Understanding and interpreting Snort configuration rules is essential for effectively customizing the behavior of the intrusion detection system. Below is an overview on how to read and comprehend Snort configuration rules.  The snort configuration rule implemented for Windows AD Server includes the following changes via notepad:     1. Change the Home Network variable:        1. Configure the output file      1. Enable the dynamic loaders      1. Enable the rule to included - in this configuration we disable all rules except for \community.rules      1. Enable the preprocessor event rules     Once these are complete, the file should be saved.   1. An additional step includes creating to list files and the White / Black listed IP addresses should be stored in these files. The snort.conf will utilise these in the IDS mode.     **More information on the Snort Rule Structure**  Snort rules follow a specific structure that consists of various components:  action protocol sourceIP/sourcePort -> destinationIP/destinationPort (options)   * Action: Specifies the action to be taken when a rule matches. Common actions include "alert," "log," or "pass." * Protocol: Specifies the network protocol being monitored, such as TCP, UDP, ICMP, etc. * Source and Destination: Specify the IP addresses and ports involved in the traffic being monitored. * Options: Additional parameters and conditions that refine the rule's behavior, such as content matching, flow control, and metadata.   **Rule Actions**  The action component of a rule determines what happens when a packet matches the rule's criteria.   * "Alert": Generates an alert message and can be accompanied by customizable information about the alert. * "Log": Logs the packet that matches the rule's criteria. * "Pass": Allows the packet to proceed without generating an alert or logging.   There are other actions available as well, depending on the version and configuration of Snort.  **Protocol and IP Address/Port Specification**   * The protocol component of a rule specifies the network protocol being monitored, such as TCP, UDP, or ICMP. * The source and destination components define the IP addresses and ports involved in the traffic being monitored. They can be specified individually or using address ranges and wildcards.   **Rule Options**  Options provide additional criteria and conditions to narrow down the rule's scope and behavior.   * Content Matching: The "content" option allows matching specific patterns or strings within packet payloads, helping identify specific threats or attacks. * Flow Control: Flow control options like "established" and "no stream" help filter traffic based on the state of the network connection. * Metadata: The "metadata" option allows adding descriptive information to the rule, such as the author, reference links, or specific details about the threat.   **Rule Modifiers and Modifiers Negation**   * Rule modifiers such as "nocase" (case-insensitive matching) and "rawbytes" (matching based on raw packet bytes) can be used to refine the rule's behavior. * Negation can be applied to modifiers using the "!" symbol to specify the inverse behavior. For example, "!nocase" would indicate a case-sensitive matching.   **Rule Classification and Priority**   * Each rule can have a classification and priority assigned to it. * Classification tags categorize the type of attack or threat the rule is designed to detect. * Priorities define the severity level of the rule, typically represented as a number from 1 (highest) to 4 (lowest).   **Rule Comments**   * Snort rules often include comments to provide additional information and context about the rule's purpose, usage, or related references. * Comments are typically preceded by the "#" symbol.   **Rule Ordering and Precedence**   * Snort processes rules in a top-down manner, evaluating each rule until a match is found. * Rule ordering and precedence matter, as a rule that matches earlier may take precedence over subsequent rules. * Ensure that the order of rules is logical and appropriate for your security requirements and network environment.   **Rule Customization**   * Snort allows customization of rules to fit specific environments and detection needs. * You can create custom rules or modify existing rules to adapt them to your network's characteristics and threat landscape. |

|  |
| --- |
| User Management |
| User roles and permissions Snort provides various user roles and permissions to manage access and control over the system. The following roles are commonly used:   * Administrator: The administrator has full control over Snort, including configuration, rule management, and user management. * Power User: Power users have elevated privileges to configure Snort and manage rules, but they may have restrictions on user management. * Read-only User: Read-only users have limited access and can only view system configurations, logs, and alerts without the ability to make changes.  Creating and managing user accounts To create and manage user accounts in Snort, follow these steps:   * Launch Snort Console: Open the Snort Console application on your Windows machine. * Access User Management: Navigate to the "Settings" or "Administration" section, where you'll find options for user management. * Create New User: Select the option to create a new user account. * Provide User Details: Enter the username, password, and email address for the new user. Ensure that the password meets the required complexity criteria. * Assign Role: Select the appropriate role (administrator, power user, read-only user) for the user. * Save Changes: Save the user account details.  Defining and assigning roles and capabilities Snort allows you to define roles and assign specific capabilities to each role. Follow these steps to define roles and assign capabilities:   * Access Role Management: Navigate to the "Settings" or "Administration" section and find the role management options. * Define Roles: Create roles such as administrator, power user, and read-only user. Specify the permissions and capabilities associated with each role. * Assign Capabilities: Determine the specific actions and features each role can access or modify. For example, administrators can configure Snort settings, manage rules, and create user accounts, while read-only users can only view logs and alerts. * Save Changes: Save the role definitions and capabilities.  Authentication options Snort offers various authentication options to control user access. These options include:   * Local Authentication: The default authentication method provided by Snort. User accounts and passwords are stored locally within the Snort system. * LDAP (Lightweight Directory Access Protocol): Allows integration with an LDAP server for centralized user authentication. Users can log in using their existing LDAP credentials. * SSO (Single Sign-On): Provides seamless authentication by integrating Snort with a Single Sign-On system such as Active Directory Federation Services (ADFS) or Security Assertion Markup Language (SAML) authentication.  To configure authentication options:  * Access Authentication Settings: Go to the "Settings" or "Administration" section and locate the authentication settings. * Choose Authentication Method: Select the desired authentication method, such as local authentication, LDAP, or SSO. * Configure Authentication Parameters: Provide the necessary details, such as LDAP server information or SSO configuration settings. * Save Changes: Save the authentication settings. |

|  |
| --- |
| Data Ingestion |
| Data Input Options:  * Snort primarily ingests network traffic data for intrusion detection and prevention. It captures and analyzes packets flowing through network interfaces. * Snort can also generate log files that contain information about alerts, events, and packet captures. These log files can be used as data input. * Additionally, Snort can integrate with other tools and systems through APIs for data input and exchange.  Configuring and Managing Data Inputs:  * Monitoring Files: Snort can monitor log files generated by itself or other tools. Configure Snort to monitor the desired log file(s) by specifying the file path in the Snort configuration file ("snort.conf"). * Network Ports: Snort monitors network traffic on specific network interfaces. Configure Snort to listen on the desired network interface(s) by specifying the interface name or IP address in the Snort configuration file. * Scripted Inputs: Snort can also integrate with scripts or custom programs to ingest data from various sources. Develop or use existing scripts to feed data to Snort for analysis.  Setting Up Sourcetypes and Automatic Field Extraction:  * Sourcetypes: Sourcetypes in Snort define the data source and format. For example, you can define a sourcetype for network traffic data and another for log files. Configure sourcetypes in your log management system or data ingestion pipeline to differentiate and classify the incoming data from Snort. * Automatic Field Extraction: Some log management systems or data ingestion tools offer automatic field extraction capabilities. Configure these tools to extract relevant fields from Snort's log data. This enables easier searching, filtering, and analysis of the ingested data.  Managing Data Input Pipelines and Sourcetypes:  * Log Management Systems: If you are using a log management system or SIEM (Security Information and Event Management) tool, configure it to receive and process the Snort logs. Define data inputs, sourcetypes, and data parsing/extraction rules within the log management system. * Data Ingestion Pipelines: If you have a custom data ingestion pipeline, design the pipeline to accept the data from Snort. Configure the pipeline to handle different data input sources (e.g., network traffic, log files, APIs) and define the necessary processing steps, such as parsing, filtering, and transforming the data. * Data Routing and Transformation: Depending on your architecture and requirements, you may need to route the Snort data to different destinations or perform data transformations. Configure your data ingestion pipeline or data processing tools accordingly to ensure the data is delivered to the intended systems or processes. |
|

|  |
| --- |
| Output Analysis |
| Snort provides a number of output files that can be analysed, the below provided an overview of the types of files and data captured to support any analysis.  Snort generates various output files that capture important information about network traffic and detected threats. The key output files include:   * Alert file: Contains detailed information about alerts triggered by Snort. * Log file: Stores information about network traffic and events captured by Snort. * Packet capture (PCAP) file: Captures network packets related to detected alerts or specified logging configurations.  Alert File Analysis: The alert file, typically named "alert.ids", contains detailed information about detected threats and triggered alerts. Each line in the alert file represents a separate alert and provides the following information:   * Date and time of the alert. * Source and destination IP addresses. * Protocol used. * Port numbers. * Classification and priority of the alert. * Description of the detected threat or attack.   Analyse the alert file to identify the types of threats detected, their severity, and the affected network hosts. Log File Analysis: The log file, usually named "snort.log", records information about network traffic and events captured by Snort. Each entry in the log file includes details such as:   * Date and time of the event. * Source and destination IP addresses. * Protocol used. * Port numbers. * Action taken by Snort (e.g., pass, alert, log).   Analyze the log file to gain insights into the network traffic patterns, the frequency of specific events, and potential security issues.  Log files are stored in ASCII and should be accessible in packet analysis software like Wireshark. These files can be opened on wireshark for better analysis. See Screenshot below:      **Packet Capture (PCAP) File Analysis:**  Snort can be configured to capture network packets related to detected alerts or based on specified logging configurations. Packet capture files, in PCAP format, contain a record of network packets for analysis with tools like Wireshark. Analyze the PCAP files to examine the actual contents of network packets related to alerts or specific events. Use packet analysis tools to inspect packet headers, payload contents, and identify any anomalies or malicious activity. |

|  |
| --- |
| Data Management |
| Snort is a network intrusion detection and prevention system and focuses primarily on real-time analysis and alerting. However, data management and retention practices can be applied to the log files generated by Snort for long-term storage and analysis. The below considerations should be considered for managing Snort Data. Indexing Configuration Snort logs can be stored in various formats, such as plain text or in a structured format like CSV or JSON. Ensure that the logging configuration is properly set to generate logs in the desired format for indexing and analysis. Managing Indexes Indexing refers to the process of organizing and optimizing log data for efficient searching and retrieval. Depending on the log analysis tool or platform you use alongside Snort, index management can vary.  Here are some general practices:   * Creation: Ensure that the logging and indexing system you use creates appropriate indexes for the log files generated by Snort. Indexes typically help speed up searches and queries. * Deletion: Define a retention policy for indexes to avoid excessive storage usage. Determine the appropriate time duration for retaining indexes based on your organization's compliance requirements and the value of historical data. * Retention Policies: Implement a retention policy that specifies the duration for which logs and indexes should be retained. This policy should align with regulatory requirements, incident response needs, and storage capacity considerations.  Data Lifecycle Management Data lifecycle management involves managing log data throughout its lifespan, including archiving, freezing, and summarization. Although Snort primarily focuses on real-time analysis, you can implement these practices for long-term storage and historical analysis.   * Archiving: Periodically archive older log files to long-term storage systems or backup solutions. This ensures that valuable historical data is retained for compliance, forensics, or analysis purposes. * Freezing: Consider freezing log data for specific time periods to prevent modification or deletion. Freezing is typically applied to logs related to ongoing investigations, litigation, or regulatory requirements. * Summarization: Depending on the log analysis tool you use, consider implementing summary indexes or accelerated data models. These techniques help condense and aggregate log data to provide higher-level insights and faster analysis.   Other advanced data modelling should be conducted on other tools utilising the data logs captured by Snort. |

|  |
| --- |
| Security and Access Control |
| Snort primarily focuses on network intrusion detection and prevention capabilities and does not have built-in security and access control features. However, there are certain areas related to securing program deployments and implementing SSL/TLS encryption that are relevant to consider when using Snort. Securing Program Deployments Firewalls and Network Restrictions: It is essential to deploy Snort in a secure network environment protected by firewalls and appropriate network restrictions. This helps control access to Snort systems and prevents unauthorized access to the network or the Snort deployment itself. User Authentication and Authorization User authentication and authorization are not native features of Snort. However, depending on the environment and deployment model, you can implement authentication and authorization mechanisms at the system level to control access to Snort configurations and logs.   * Local Authentication: If Snort is deployed on a system with user accounts, you can leverage the underlying operating system's authentication mechanisms for user access control. * LDAP Integration: You can integrate Snort with an LDAP (Lightweight Directory Access Protocol) server to authenticate and authorize users based on a centralized user directory. This allows for centralized user management and access control across multiple Snort instances. * Single Sign-On (SSO): If your organization uses a single sign-on solution, you can integrate Snort with the SSO system to enable seamless authentication and access control based on the organization's user identity management framework.  Role-Based Access Control (RBAC) and Permissions Snort itself does not offer RBAC or granular permissions management. However, you can utilize the underlying operating system's permissions and access control mechanisms to enforce role-based access control and assign appropriate privileges to users accessing Snort configurations, log files, or associated resources. Implementing SSL/TLS Encryption for Data in Transit To ensure the confidentiality and integrity of data transmitted between Snort components or other systems, it is recommended to implement SSL/TLS encryption. SSL/TLS can be used to secure communication channels between Snort sensors, management consoles, or data storage systems. |

|  |
| --- |
| Maintenance and Upgrades |
| Snort, being an open-source network intrusion detection and prevention system, does not provide built-in maintenance and upgrade features. However, as a security tool, it is essential to consider certain maintenance and upgrade practices to ensure the effective and secure operation of Snort. Routine Maintenance Tasks  * Log Rotation: Implement a log rotation mechanism to manage the size and storage requirements of Snort's log files. This ensures that logs are efficiently managed and storage space is optimized. * Data Grooming: Regularly review and remove outdated or irrelevant log data to maintain the efficiency and effectiveness of log analysis.  Applying Updates and Patches Snort, like any software, may release updates and patches to address bugs, security vulnerabilities, or introduce new features. It is crucial to stay updated with the latest releases and apply updates and patches promptly to maintain the security and stability of Snort.In is important to monitor the Snort community, official website, and mailing lists to stay informed about new releases and security advisories. Backup and Disaster Recovery Procedures Implement regular backups of Snort's configuration files, rule sets, and any other relevant data. This ensures that you have a recovery point in case of system failures or the need to restore Snort to a previous state. Like many other security systems the standard backup strategies should be implemented and consider off-site storage options for critical backups to protect against data loss or disasters. Version Compatibility Considerations and Upgrade Planning When planning upgrades, consider the compatibility of Snort with your underlying operating system, network infrastructure, and any related tools or plugins you may be using. It is important to review release notes and documentation to understand any specific considerations or requirements for upgrading Snort to newer versions.  It is recommended to test upgrades in a non-production environment before deploying them in a live environment to identify and address any compatibility issues or conflicts. |

|  |
| --- |
| Resources and References |
| Below is a list of references and resources to support the use of Snort: Snort Official Documentation: The official documentation provides comprehensive information about Snort's installation, configuration, and usage. It also covers advanced topics and features. You can access it at: https://www.snort.org/documents  **Snort Release Notes**:  The release notes provide details about new features, bug fixes, and known issues in each Snort release. They can be found on the Snort website or in the documentation section.  **Snort Community Forum**:  The Snort community forum is a valuable resource to connect with other Snort users, ask questions, and get support. You can visit the forum at: https://forum.snort.org/  **Snort Mailing Lists**:  Snort maintains several mailing lists where users can discuss topics, ask questions, and share knowledge. You can find more information about the available mailing lists on the Snort website.  **Snort Blog**:  The Snort blog provides updates, news, and in-depth articles related to Snort and network security. It covers topics such as new features, best practices, and real-world use cases. You can access the blog at: <https://www.snort.org/blog>  **Snort Rule Repositories**:  Several online repositories host community-contributed Snort rules that you can study and use as references. These repositories often include rules for specific threats, emerging vulnerabilities, and common attack patterns. Some popular repositories include Emerging Threats (www.emergingthreats.net) and Open Information Security Foundation (OISF) Suricata rules (suricata-ids.org/rules). |