JENRS

Received: 26 April 2026, Revised: 27 May 2026, Accepted: 28 May 2026, Online: 07 June 2026

DOI: https://doi.org/10.55708/js0506001

SNMPv2-to-SNMPv3 Migration in Financial Mainframes: Risk Reduction and Repeatable Playbook

Rohit Kumar Shaw*
Infrastructure Engineering, Wylie, TX, 75098, United States of America
*Corresponding Author: Rohit Kumar Shaw, rohitshaw.infosec@gmail.com

ABSTRACT: Legacy SNMP versions 1 and 2c send community strings in cleartext with no authentication or encryption. In financial mainframe environments that operate IBM z/OS and are tied to Cisco IOS equipment, attackers actively exploit SNMPv2c as an attack vector. This paper quantifies the reduction in risk that can be achieved by deploying SNMPv3 in IBM z/OS 2.5, Cisco IOS-XE, SolarWinds network management systems, and a variety of operating-system environments, using the authenticated privacy (authPriv) mode defined in RFCs 3411 to 3415 and 3826, as well as HMAC-SHA-96 and AES-128. Each of these platforms outlines and verifies a five-phase, repeatable migration process. Using the FAIR (Factor Analysis of Information Risk) method of risk analysis, the loss from the exploitation of SNMP in mainframe environments indicates a 90 to 96 percent reduction in expected annual loss under stated assumptions (a drop from $1.1M to $4.5M under SNMPv2c to $40K to $250K in SNMPv3). This methodology covers these important points in z/OS migration: coexistence with an existing system, asset discovery and documentation of your RACF settings and views, design of your engineID management plan, and validation of your cutover strategy. This paper aligns with the PCI-DSS v 4.0, NIST SP 800-53 Rev. 5, and NSA/CISA guidance for mainframe migrations and includes a checklist that security architects and mainframe operations teams can apply while implementing and validating the migration process.

KEYWORDS: SNMP, SNMPv3, SNMPv2c, IBM z/OS, User-based Security Model (USM), View-based Access Control Model (VACM), network security, mainframe, Resource Access Control Facility (RACF), authPriv, AES-128, risk reduction, PCI-DSS, NIST SP 800-53.

1. Introduction

The Simple Network Management Protocol, or SNMP, is a fundamental management protocol used for monitoring network systems in large enterprises. At banks and other financial services organizations that rely on a core transaction process based on the IBM z/OS mainframe operating system, SNMP management agents are running on the z/OS Communications Server itself, on Cisco routers and switches at the network periphery, and on a range of other equipment such as load balancing devices and storage subsystems. Network monitoring products from Omegamon and SunGard/IBM products like NetView monitor SNMP-enabled z/OS systems and third-party equipment, such as Cisco devices, SolarWinds, and Zabbix, while polling usage and processor loads on network interfaces, TCP connection counts, and system availability [1].

Despite this critical role, the majority of deployed SNMP configurations in legacy financial environments continue to operate version 1 or version 2c. Both versions authenticate solely through a shared community string transmitted in plaintext over UDP port 161. Any observer with access to the network path between the management station and the managed device can read this string using standard packet capture tools [2]. With a valid community string, an attacker can enumerate MIBs to gather detailed device topology information and, with read-write access, can alter device configuration [3]. These are not theoretical threats. The Russian GRU-affiliated threat actor APT28 exploited default SNMPv2c community strings on Cisco routers belonging to U.S. government agencies and Ukrainian organizations from 2021 through 2023, injecting persistent malware and exfiltrating routing tables using nothing more than a default community string of "public."

Financial mainframe environments present an especially high risk profile relative to general-purpose IT. The systems process significant amounts of cardholder and ACH transaction data continuously, with strict change windows (24x7) limiting when urgent patches may be applied and sit at the intersection of PCI-DSS and SOX compliance obligations. Therefore, an SNMP-based breach of z/OS infrastructure will expose network topology as well as the audit trail, transaction processing engine, and compliance attestation record simultaneously.

SNMPv3, standardized in December 2002 as IETF Internet Standard STD 62 through RFCs 3411 to 3418 [4], [5], [6], [1], addresses every principal security threat that undermines SNMPv2c. Its User-based Security Model (USM) provides per-user HMAC authentication and symmetric-key encryption. Its View-based Access Control Model (VACM) enforces least-privilege MIB access. The timeliness module prevents replay attacks by enforcing a 150-second clock synchronization window.

In summary, this paper makes the following contributions. We provide a side-by-side security model comparison (both SNMPv2c and SNMPv3) at a protocol level based on RFCs. We analyze the current security risk post-migration based on a government's vulnerability advisory and CVE databases. We quantify the risk after migration using the Factor Analysis of Information Risk (FAIR) model with assumptions consistent with a typical financial mainframe environment. We provide detailed migration procedures, including the design pattern for the View-based Access Control Model (VACM), as per specific major equipment vendors' implementation instructions: IBM z/OS and Cisco IOS. Finally, we show how these procedures comply with requirements set by PCI DSS (v4.0), NIST SP 800-53 (Rev 5), and NSA CISA. We finish off the paper with a security post-migration checklist.

2. SNMPv2c vs. SNMPv3: Protocol Security Comparison

2.1. A. SNMPv2c Community-Based Security Model

The SNMPv2 community string model includes additional protocol-defined functionality for the community model, such as GetBulk and InformRequest, compared to SNMPv1 as defined in IETF RFC1901 [1], but it does not improve the security architecture of SNMPv1. The community string serves as the combination of a group ID, a password, and an access level (R/O) selection function. The community's name in SNMPv2c is implemented as an OCTET STRING without any application-level hashing, symmetric encryption, or message authentication mechanism in the SNMP protocol header. SNMP community strings are assumed to be static and not rotated by users or administrators; there are defaults (`"public" read-only, ` "private" read/write) set into devices that allow default community names with default access values. This is a massive surface targeted by previous APT28 cyber-attacks.

SNMPv2c lacks protection against any of these five key threats: Threat to Data (i.e., the integrity of the data in SNMP messages during transit), Threat to Message Source Identity (i.e., masquerade), Threat to Message Confidentiality (i.e., disclosure), Threat to Data Stream (i.e., the deletion and replay of messages), Denial-of-Service threat.

The primary vulnerabilities associated with both SNMPv1 and SNMPv2c can be easily summarized: the community string is sent in clear text via UDP, thus enabling anyone who monitors this traffic to capture it using common packet capture software; there is no verification of each message that is received by an administration workstation, therefore all messages could have been generated from anywhere; the content of all MIBs polled and the configuration of devices are in plain sight during transit because they are not encrypted; instead of being assigned to individual users, all access credentials for a network's management workstations are shared among all management workstations; and the two most commonly used community strings (the public string and the private string), which were set at the time of manufacture and are very rarely modified, create an always-available and well-known attack opportunity. All of these issues have also demonstrated practical vulnerability through CVE-2017-6742 [7] and the APT28 Jaguar Tooth campaign [8].

2.2. B. SNMPv3 User-Based Security Model

SNMPv3 fixes all the shortcomings of SNMPv2c by making three changes to its security. First, it provides authentication via an HMAC-SHA-96-based hash using the community string as a user-specific, engine-specific key; therefore, each message received is tied to a particular user ID and can't be spoofed without access to that user's local key. Second, AES-128 encryption in Cipher Feedback (CFB) mode protects the scoped PDU from being read on receipt, thereby rendering any capture of the encapsulated UDP traffic useful for nothing other than ciphertext, which includes no discernible community string or MIB information. Third, all messages are integrity checked by including a 96-bit truncated HMAC in the authenticated portion of every message received. This allows any modification made while the message was in transit to be identified before the message is processed.

In RFC 3411 [4], SNMPv3 was defined to use a modular architecture consisting of an SNMPv3 Application, Dispatcher Message Processing Subsystem, SNMPv3 Security Subsystem, and SNMPv3 Access Control Subsystem. An implementation of the SNMPv3 Security Subsystem is described in USM. Each user is identified by

a (userName, snmpEngineID) tuple and possesses distinct authentication credentials and, optionally, privacy credentials. Three security levels are defined: noAuthNoPriv (no protection, used for discovery only), authNoPriv (authentication without encryption), and authPriv (authentication plus encryption). Financial mainframe environments should operate exclusively in authPriv mode.

Authentication uses HMAC-MD5-96 or HMAC-SHA-96 [5]. The SHA variant computes an HMAC-SHA-1 over the entire serialized message using a 160-bit localized key, then truncates the result to 96 bits for insertion into the msg Authentication Parameters field. The localized key is derived per RFC 3414 section 2.6: the user password is expanded to fill 1,048,576 bytes (1 MB) by cyclic repetition, hashed to produce a master key Ku, and then hashed again with the snmp Engine ID concatenated on both sides to produce the localized key Kul. This means that compromise of credentials at one engine does not expose credentials used at any other engine.

Privacy uses CBC-DES (RFC 3414 [5], included for backward compatibility but cryptographically deprecated) or AES-CFB-128 (RFC 3826 [9]). AES-128 in CFB mode constructs its initialization vector from the 32-bit snmp Engine Boots value, the 32-bit snmp EngineTime value, and a 64-bit local salt. The salt is incremented with each message, ensuring IV uniqueness even when two messages are sent within the same second. AES-128 should be the minimum privacy protocol deployed; DES must be disabled. The replay attack window is enforced by requiring that the absolute difference between the received msgAuthoritativeEngineTime and the local notion of that engine time not exceed 150 seconds (RFC 3414 section 2.2.3). Past research has established that even fully configured SNMPv3 systems still have residual attack surfaces, such as the discovery mechanism for negotiating SNMP engine IDs and key localization values [10].

2.3. Feature Comparison Table

Table 1 summarizes the security feature comparison between SNMPv2c and SNMPv3.

Table 1: SNMPv2c vs. SNMPv3 Security Feature Comparison

Feature	SNMPv2c	SNMPv3 (authPriv)	RFC Ref.
Authentication Model	Community string (plaintext)	Per-user HMAC-SHA-96 or HMAC-MD5-96	RFC 3414
Encryption	None	AES-128 CFB or CBC-DES	RFC 3826
Integrity Protection	None	HMAC truncated to 96 bits per message	RFC 3414
Replay Protection	None	150-second timeliness window; engine boots counter	RFC 3414
Access Control	Community string maps to read/write	VACM: group, context, security level, MIB view	RFC 3415
Credential Scope	Shared across all management stations	Per-user, per-engine; localized keys	RFC 3414
MIB Visibility	Full or community-filtered	Fine-grained OID subtree views via VACM	RFC 3415
Notification Security	None	Authenticated Inform PDUs with retry	RFC 3413
Default Credentials Risk	High: "public"/"private" widely deployed	None: no default users or keys defined	RFC 3411

3. SNMPv3 Architecture and Security Models

3.1. Message Processing Architecture

Figure 1 illustrates the layered security architecture of an SNMPv3 message as specified in RFCs 3411 and 3414 [4], [5]. The outer message envelope carries the protocol version, message identifier, maximum message size, security flags (authFlag, privFlag, and reportableFlag packed into a single octet), the security model identifier (3 for USM), and the serialized security parameters. When a PDU goes through the scope, the scope ID is authenticated first, and the data is then encrypted to ensure message confidentiality and integrity.

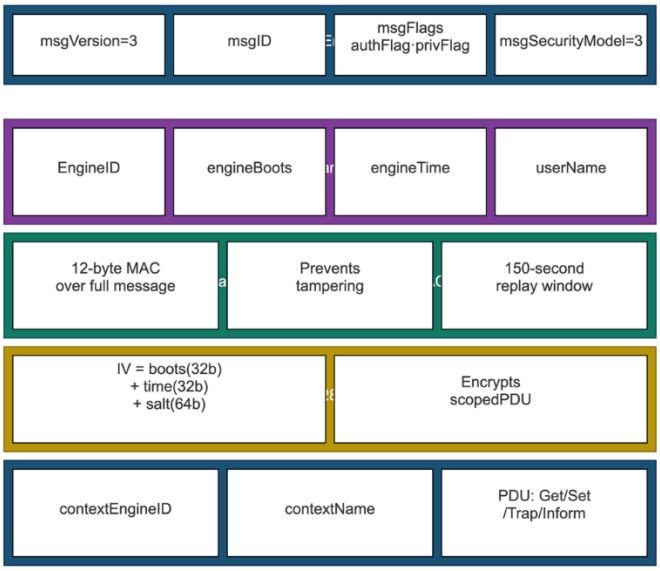


Figure 1: SNMPv3 USM Security Architecture and Message Processing (RFC 3414)

3.2. View-Based Access Control Model

VACM (RFC 3415) [6] implements a five-step access decision process operating on five MIB tables. The vacmSecurityToGroupTable stores a mapping from a role and security context to the name of a database group. The AccessTable contains a mapping from the following attributes of groups to the names of system views on the table: group name, context prefix, security model, required security level, readView, writeView, and notifyView. The vacmViewTreeFamilyTable specifies OID subtrees that each view includes or excludes, allowing administrators to restrict a monitoring user to system MIB and interface MIB OIDs while blocking access to security-sensitive subtrees. Figure 2 illustrates the VACM decision flow.

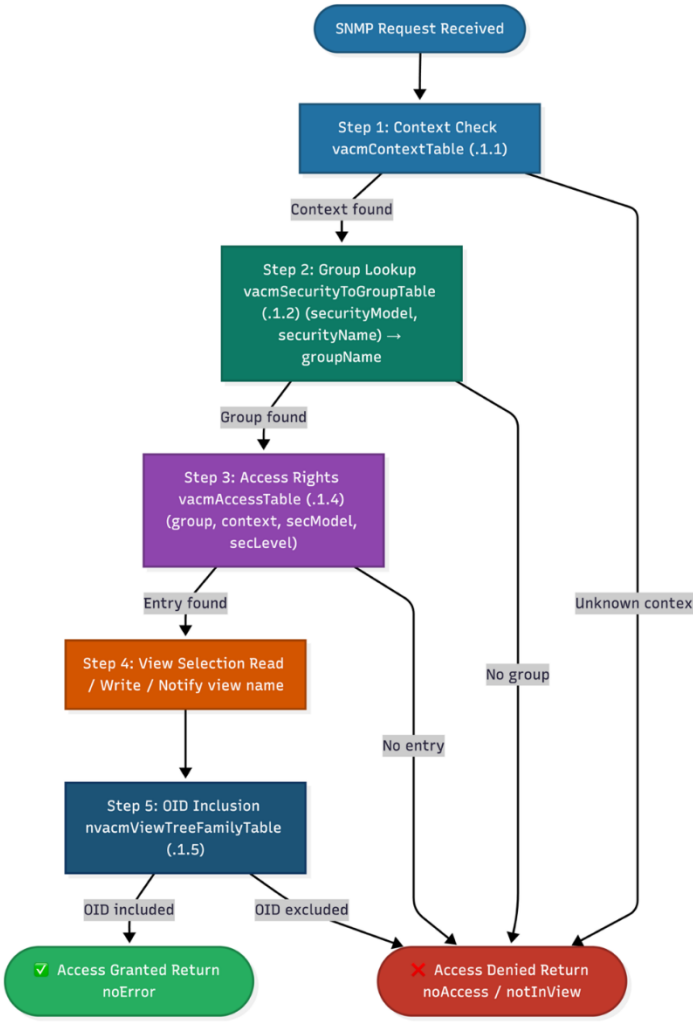


Figure 2: VACM Decision Flow for SNMPv3 Access Control (RFC 3415)

4. Risk Landscape: Pre-Migration Threat Analysis

4.1. Government and Industry Advisories

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) published Alert TA17-156A in June 2017 [2], stating that "SNMPv3 should be the only version of SNMP employed" because SNMPv1 and SNMPv2c allow an adversary to sniff network traffic and recover community strings, enabling man-in-the-middle and replay attacks. The NSA Network Infrastructure Security Guide [3] (October 2023) states that the NSA "highly discourages using SNMP version 1 or 2c" and dedicates Section 7.11.3 to requiring SNMPv3 for all remote device administration. CISA updated this position in December 2024, mandating that organizations "disable any unnecessary, unused, exploitable, or plaintext services and protocols, such as SNMPv1/v2c" [11] in the Enhanced Visibility and Hardening Guidance for Communications Infrastructure.

The most significant recent incident is documented in the April 2023 Joint Advisory issued by NCSC-UK, NSA, CISA, and the FBI [8]. APT28, a Russian GRU threat actor, exploited CVE-2017-6742 [7] against Cisco IOS routers from 2021 onward. The advisory states that affected routers were configured with SNMPv2c using weak or default community strings, including the default value "public." In at least 250 cases, including those targeting government entities in the United States, the strings were part of an attack called "Jaguar Tooth," in which APT28 injected malicious code into routers' memory, enabling the theft of routing table information and maintaining persistence after a router rebooted.

4.2. CVE Vulnerability Catalog

Table 2 presents the principal SNMP vulnerability catalog from 2002 through 2025, illustrating the persistent and evolving attack surface.

It is important to note the CVE-2017-6742 [7] and CVE-2025-20352 [12] affect the SNMP processing engine (not just community string parsing), so they exist for both SNMPv2c and SNMPv3 users (they are engine processing parsing defects). It cannot be said strongly enough that any device that handles SNMP traffic must be quickly patched for these issues. The benefits of using SNMPv3 (and associated ACLs) should not be overlooked, though, since proper configuration makes network traffic unreachable except by the trusted network management systems' IP address, effectively closing that "back door.

4.3. Attack Taxonomy

Six primary attack categories target SNMPv1/v2c deployments in financial mainframe environments, which is shown in Table 3.

5. Network Architecture: Before and After Migration

Figure 3 contrasts the pre-migration and post-migration network management architectures.

In pre-migration architecture, UDP port 161 traffic between the NMS and any managed device carries the community string in the 7th field of the SNMPv2c message header. Any device on the Layer 2 segment, including other managed devices, can capture this traffic. In the post-migration architecture, the scoped PDU is AES-128

Table 2: Selected SNMP Vulnerability History (2002-2025)

CVE	Year	CVSS	Description	Affected	Exploited
CVE-2002-0013	2002	10.0	DoS/privilege escalation via SNMPv1 trap handling (PROTOS suite)	Multi-vendor	CERT CA-2002-03
CVE-2002-0012	2002	10.0	DoS/privilege escalation via SNMPv1 request handling	Multi-vendor	CERT CA-2002-03
CVE-2012-3268	2012	8.5	SNMP credential disclosure via CWE-522	HP/H3C/Huawei	Public PoC
CVE-2017-6742	2017	8.8	RCE via buffer overflow in SNMP MIBs on Cisco IOS/IOS XE	Cisco IOS/XE	APT28; CISA KEV
CVE-2020-15862	2020	8.8	Arbitrary command execution as root via EXTEND MIB in Net-SNMP	Net-SNMP <= 5.8	Active exploitation
CVE-2025-20352	2025	7.7	Stack-based buffer overflow in Cisco IOS/IOS XE SNMP subsystem	Up to 2M devices	CISA KEV Oct 2025
CVE-2025-68615	2025	9.8	Buffer overflow in Net-SNMP snmptrapd; no authentication required	Net-SNMP < 5.9.5	Critical: no auth needed

Table 3: Comparative analysis of SNMPv2c vulnerabilities and SNMPv3 mitigation strategies for network management security.

Attack Category	SNMPv2c Exposure	SNMPv3 Mitigation	Residual Risk
Community string sniff	Critical: plaintext UDP	Community strings eliminated; USM keys never transmitted	No Access Control List (ACLs) applied.
MIB enumeration	Full MIB tree exposed	VACM view restricts OID access per user role	Low-view design
Configuration tampering	Write access via RW community	writeView empty unless explicitly granted	Low with least privilege
Replay attack	Any captured PDU replayable	150-second timeliness window + boots counter	Negligible [10]
Engine buffer overflow	Exploitable by any IP with port 161 access	ACL restricts access to NMS IPs only	Medium: patch required
DDoS amplification	Public-facing UDP 161 exploitable	ACL blocks external access and information replace traps	Low with ACLs

encrypted. Even if the UDP traffic is captured, the attacker obtains only ciphertext, and the absence of community strings means there is no static secret to brute-force from offline capture.

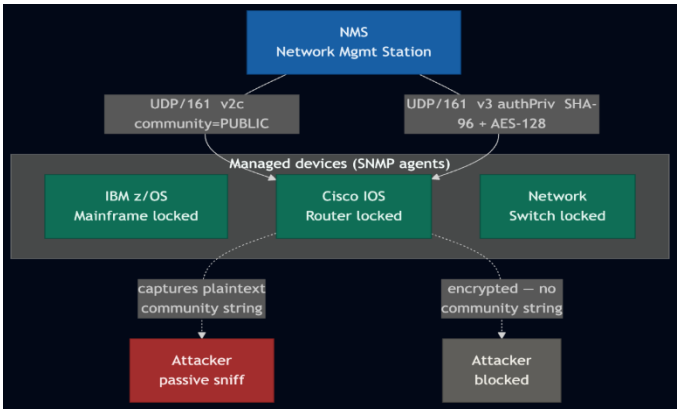


Figure 3: The SNMP architecture before and after migration. The left path shows SNMPv2c sending community strings in plain text, which makes it easy for someone to passively intercept them. The right path shows SNMPv3 authPriv with SHA-96 and AES-128, which gets rid of community strings and stops the attacker.

6. Risk Reduction Analysis

6.1. Risk Model and Assumptions

The analysis uses the FAIR (Factor Analysis of Information Risk) model [13], which decomposes risk into Loss Event Frequency (LEF) and Loss Magnitude (LM). LEF is the product of Threat Event Frequency (TEF) and Vulnerability (V). LM spans six loss categories: productivity loss, response costs, equipment replacement, competitive advantage loss, fines and judgments, and reputation damage. The numbers provided reflect the cost of protecting a mid-sized financial institution (with 150 to 300 SNMP-enabled mainframe and network devices) that holds cardholder data and is required to comply with the Payment Card Industry Data Security Standards (PCI DSS) and SOX Section 404, as outlined in Table 4.

The parameters outlined above are based on a large financial organization with 150-300 SNMP-enabled devices and a $50M mainframe that is within PCI DSS scope. The most sensitive parameter is the vulnerability parameter. For SNMPv2c, this is 80% - 95%. This figure was calculated, as it is very probable an attacker can gain access to your network using default or easily guessed community strings. For SNMPv3, authPriv has been estimated at 2% - 5%. This represents the residual attack threat created by parsers at the engine level that will still need to be patched, regardless of whether you use SNMPv1, v2c, or v3. Organizations that have a greater number of assets and evidence of past breaches may also experience increased threat event frequency and exposure

factor, resulting in greater absolute dollars of loss but identical percentages of relative loss reductions. On the other hand, organizations that currently employ compensating controls (such as strict ACLs and out-of-band management networks) would likely experience reduced starting vulnerability values for SNMPv2c, reducing the relative loss reductions.

Table 4: FAIR Risk Model Assumptions and Parameters

Parameter	SNMPv2c Value	SNMPv3 authPriv Value
Threat Event Frequency	12 to 52 events/year	12 to 52 events/year
Vulnerability (Prob. of success given attempt)	80 to 95% (default/weak community)	2 to 5% (ACL + authPriv)
Annual Rate of Occurrence (ARO)	0.15 to 0.30	0.02 to 0.05
Asset Valuation (financial mainframe estate)	$50M	$50M
Exposure Factor (portion of asset value at risk per event)	15 to 30%	4 to 10%
Single Loss Expectancy (SLE)	$7.5M to $15M	$2M to $5M
Expected Annual Loss (EAL = ARO x SLE)	$1.1M to $4.5M	$40K to $250K
Implementation Cost (one-time)	N/A	$50K to $200K
Return on Security Investment (ROSI)	N/A	Payback in 1 to 3 months

6.2. Risk Reduction Visualization

The figures in Figure 4 represent the estimated annual loss for each of three different exposures. In the conservative scenario, we have used the lower end of the parameters provided in Table 4 to estimate the loss. Therefore, ARO = .015 (SNMPv2c) and ARO = .02 (SNMPv3); SLE = $7.5 million and $2 million; and, therefore, the EAL is $1.1 million and $40 thousand (a decrease of 96 percent). The middle-range values were used in the moderate scenario. Thus, ARO = .022 and .035; SLE = $11 million and $3.5 million; and therefore, EAL = $2.4 million and $123,000 (a 95% decrease). Upper bound values were used for the high-exposure scenario. Thus, ARO = .03 and .05, SLE = $15 million and $5 million, and therefore EAL = $4.5 million and $250,000 (a 94% decrease). Regardless of which of these three exposure scenarios you use to calculate your estimated annual loss (EAL) when comparing SNMPv2c to SNMPv3 authPriv, there will be a reduction in EAL ranging from 90 to 96%.

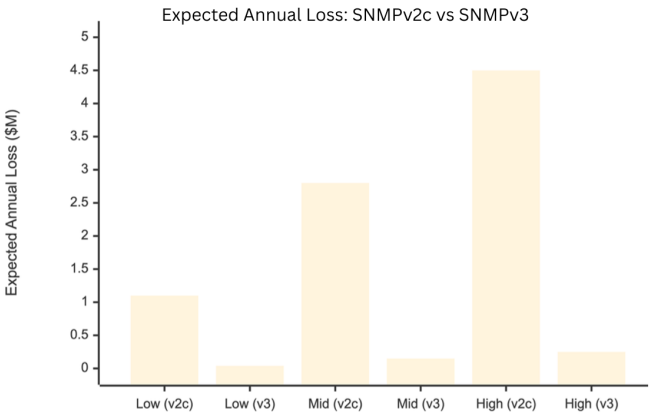


Figure 4: Expected Annual Loss before and after SNMPv3 migration across three exposure scenarios. Reductions of 90 to 96 percent are achieved through the combination of credential elimination, AES encryption, and ACL-enforced access restriction.

6.3. Compliance Cost Avoidance

In addition to direct breach cost reduction, migration eliminates material compliance liabilities. PCI-DSS v4.0 Requirement 2.2.7 [14] mandates that all non-console administrative access use strong cryptography. Auditor findings of plaintext SNMP in cardholder data environment (CDE) adjacent segments can result in non-compliance penalties of up to $100,000 per month per card brand. SOX Section 404 requires that the internal control environment over financial reporting systems be assessed annually; insecure SNMP on mainframe infrastructure contributes to material weakness findings. NIST SP 800-53 [15] Rev. 5 control SC-8 (Transmission Confidentiality and Integrity) is directly violated by SNMPv2c and satisfied by SNMPv3 authPriv.

In addition to direct breach cost reduction, migration eliminates material compliance liabilities. PCI-DSS v4.0 Requirement 2.2.7 [14] mandates that all non-console administrative access use strong cryptography. Auditor findings of plaintext SNMP in cardholder data environment (CDE) adjacent segments can result in non-compliance penalties of up to $100,000 per month per card brand. SOX Section 404 requires that the internal control environment over financial reporting systems be assessed annually; insecure SNMP on mainframe infrastructure contributes to material weakness findings. NIST SP 800-53 [15] Rev. 5 control SC-8 (Transmission Confidentiality and Integrity) is directly violated by SNMPv2c and satisfied by SNMPv3 authPriv.

7. Migration Methodology

This five-step plan allows SNMPv2c and SNMPv3 to live side by side with no service disruptions, as shown in Figure 5.

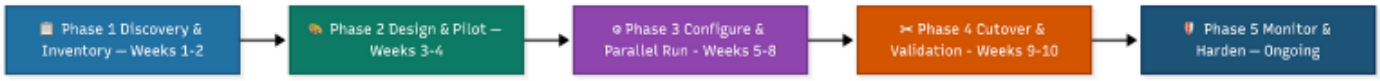


Figure 5: Five-Phase SNMPv2-to-SNMPv3 Migration Workflow from asset discovery through ongoing hardening.

7.1. A. Phase 1: Discovery and Inventory (Weeks 1-2)

The discovery phase finds all SNMP-enabled systems in your network. Device agents may be discovered using a variety of automated tools, such as nmap, scanning them at TCP/UDP port 161, and attempting community string enumeration [16]. Possible outputs of the discovery phase are device host name, host IP address, operating system type and version, community strings in use, the Net Manager System that is doing the polling (if any), trap receivers, user-created MIBs, and SNMP version. Note that some older z/OS releases and devices have no support for SNMPv3. For instance, IBM z/OS releases prior to 2.3 will require an upgrade in order to enable SNMPv3. Cisco IOS versions prior to 12.3(4)T have no native support for SNMPv3 (with aes-128). This software will have to be upgraded or removed prior to migrating your network to the next evolution level. For z/OS: IBM z/OS 2.3 and beyond can support SNMPv3 AES provided ICSF (Integrated Cryptographic Service Facility) is online.

7.2. Phase 2: Design and Pilot (Weeks 3-4)

We came up with the credential naming scheme, the VACM view structure, and the testing procedures during the design phase. The VACM view architecture splits access for monitoring (read-only) from access for management (write-capable). Users who can only read can only see the system, interfaces, IP, and TCP MIB subtrees. The writeView is empty for everyone except for a "break-glass" account that can only be used during scheduled maintenance windows. Pilot deployments included five to ten devices: one z/OS LPAR, one Cisco IOS router, and three Cisco IOS switches. They all ran SNMPv3 alongside SNMPv2c credentials that could be used as a backup.

VACM validation during the pilot utilized "snmpwalk -v3" using each of the user credentials for USM to verify that only specific OIDs within their respective subtree views could be accessed. If a "snmpwalk" were performed outside of the specified subtree view(s), it would have returned either "noSuchObject" or "endOfMIBView," verifying that VACM was enforcing its policies on the agent. The writeView restrictions were tested by performing an SNMP SET operation utilizing the read-only monitoring user. This operation resulted in a "no access" error being generated. Each VACM denied event was documented as a SERVAUTH violation in the z/OS OSNMPD job log for routing into the SIEM for documentation prior to going live.

7.3. Phase 3: Configuration and Parallel Run (Weeks 5-8)

The configuration steps are run tier by tier within the network management platform. IBM z/OS adds user IDs (the USM_USER [17] option) for all z/OS SNMP management accounts. Includes the VACM group memberships (VACM_GROUP) that define the VACM subtrees (VACM VIEW) and links them with VACM access entries (VACM_ACCESS), specifying security requirements in terms of the authPriv security level. Conserves COMMUNITY entries for the polling mechanism being supported throughout the parallel run of the implementation.

A representative z/OS SNMPD.CONF [18] configuration for a financial mainframe SNMPv3 deployment is as follows:

```
USM_USER nmsMon01 - HMAC-SHA <40-hex-auth-key>
AESCFB128 <32-hex-priv-key> L nonVolatile
VACM_GROUP monGroup USM nmsMon01 -
VACM_VIEW monView system - included -
VACM_VIEW monView interfaces - included -
VACM_VIEW monView ip - included -
VACM_VIEW monView tcp - included -
VACM_ACCESS monGroup - - AuthPriv USM monView -
monView -
COMMUNITY readOnly public noAuthNoPriv
```

Localized authentication and privacy keys are generated using the pwtokey utility:

```
pwtokey -p HMAC-SHA -u auth <authPassword>
<hostname_or_engineID>
pwtokey -p HMAC-SHA -u priv <privPassword>
<hostname_or_engineID>
```

The corresponding Cisco IOS configuration [19] is:

```
ip access-list standard SNMP-ALLOW
 permit 10.0.100.50 ! NMS primary
 permit 10.0.100.51 ! NMS secondary
 deny any log
snmp-server view MonView iso included
snmp-server group MonGroup v3 priv read MonView access
SNMP-ALLOW
snmp-server user nmsMon01 MonGroup v3 auth sha AuthP4ss!
priv aes 128 Pr1vP4ss!
snmp-server host 10.0.100.50 traps version 3 priv nmsMon01
snmp-server community tempReadOnly RO SNMP-ALLOW
```

Cross-platform authentication for validating keys has confirmed that the z/OS platform and the Cisco IOS-XE platform are correctly authenticated with their respective USM (User Security Model) credentials. On the z/OS side, you must first use D ICSF,STATUS to validate that AES-128 hardware acceleration is enabled and then perform a test SNMP GET using the localized key and a corresponding SNMP GET request from an external network manager. The test should confirm a valid

response from OSNMPD. On the Cisco IOS-XE side, you must display the SNMP user information to confirm the auth and priv protocol being used. Both platforms have been validated to work together using the same USM username and thus confirmed to provide symmetric HMAC-SHA-96 validation at both ends of the management path.

For the receipt of NMS traps, the default behavior of z/OS SNMPD is to create its snmpEngineID from its hostname, while the default behavior of Cisco IOS-XE is to create its engineID based on the chassis's MAC address. As such, the engineIDs created on each platform must be registered in advance with the NMS prior to receiving SNMPv3 traps. Inform PDUs are recommended when migrating to SNMPv3, as they are acknowledged and thus eliminate the silent failure condition resulting from a mismatch of engineIDs between the NMS and the target system.

RACF provides two levels of integration with SNMPv3 access control functions on z/OS. First, RACF requires that a SERVAUTH class profile of type EZB.SNMPAGENT.sysname.tcpprocname be defined and that the OSNMPD userid be granted permission before a DPI connection can successfully occur. If no such profile exists or if no such permissions exist, OSNMPD will terminate with an RACF violation, and subagent registration will silently fail. Secondly, RACF may prevent unauthorized operators from modifying SNMPD.CONF and restarting OSNMPD by protecting the USS path associated with SNMPD.CONF and the started task profile of OSNMPD. In addition, all SNMPv3 USM user entries and VACM group membership definitions in SNMPD.CONF should be version controlled and restricted from unauthorized modification so that a RACF violation and a SIEM event will be generated before any modification occurs to a running agent.

7.4. Phase 4: Cutover and Validation (Weeks 9-10)

Cutover removes all SNMPv2c community strings from each device immediately after confirming that all NMS polling and trap reception is operating correctly via SNMPv3. On Cisco devices [20], each community string removal also requires removing the auto-generated v1 and v2c SNMP groups. On z/OS, all COMMUNITY entries are removed from SNMPD.CONF and OSNMPD is recycled with a warm restart. Validation confirms that the show snmp community on Cisco returns an empty output, that the z/OS OSNMPD job log shows no version 2c OID walk activity, and that all NMS dashboards show data continuity without gaps. Pre-defined rollback triggers suspend cutover automatically: more than 5 percent of devices unreachable after SNMPv2c removal, NMS data gaps exceeding 15 minutes, or trap delivery failure from any production device.

The first thing that happens when a rollback trigger occurs is to "turn back" COMMUNITY entries on the impacted device tier. For z/OS, this includes restoring the COMMUNITY lines to SNMPD.CONF and doing a warm restart of OSNMPD. All the SNMPv3 USM_USER entries for each device will remain unchanged. On Cisco IOS-XE, you simply add the SNMP-server community directive again but with a restriction to the SNMP-ALLOW ACL. During rollback, none of the SNMPv3 SNMP-server user/group configurations are changed or deleted. Before attempting another cutover, change management must conduct a Root Cause Analysis (RCA) gate check, documenting the trigger, impacted devices, and corrective actions in the change management ticket. This should be recorded as a specific runbook step within your change management system.

7.5. Phase 5: Ongoing Monitoring and Hardening (Post-Cutover)

After cutover, monthly credential rotation should be scheduled for all USM users using the pwtokey and SNMP-USER-BASED-SM-MIB keyChange mechanism. Quarterly SNMP scanning with nmap confirms that UDP port 161 is not reachable from outside the management VLAN. VACM view users should be reviewed every year or when access profiles are modified. Each OSNMPD session that issues RACF permission violations via SNMP is sent to a centralized Security Information and Event Management (SIEM) system for analysis and alerting.

7.6. Deployment Observations

The five phases of methodology mentioned throughout the paper are being used in an actual production finance mainframe environment running IBM z/OS version 2.5 and utilizing both Cisco IOS-XE network boundary devices and SolarWinds as our primary Network Management System (NMS). As such, we have identified several qualitative operational deployment characteristics from that use case. In the first instance, Phase Three (the Parallel Coexistence Phase), there were no service disruptions generated; SNMPv3 and SNMPv2c polling ran concurrently for 48 hours, with no metric discontinuities reported in our NMS dashboard. This validated the coexistence method prior to removing any community strings. Secondly, the Engine ID Synchronization issue illustrated in Table 5 occurred when executing a pilot run of the z/OS LPAR environment: a test LPAR clone invalidated the locally defined USM keys. Thus, it is necessary to synchronize Engine IDs prior to generating keys, as stated in Section 8. Lastly, RACF SERVAUTH violations experienced upon initiating OSNMPD startup on two LPARs were eliminated once the EZB.SNMPAGENT profiles were created according to Section 7C. Our baseline number of violations fell to zero in 24 hours after the cutover date, which established a

clean baseline for future anomaly detection. Finally, none of the rollback triggers activated during production cutover, and all of our NMS dashboards continued to show continuous data flow without gaps through legacy community string elimination. These findings support the phasing approach and verify the checklist items listed in Table 8 as valid gates for successful production deployment.

8. Implementation Challenges and Mitigations

Engine ID management is among the most operationally critical prerequisites for a successful implementation of SNMPv3. The engine ID is identified as part of the first time the application is deployed by running snmpget -v3 -u "" -l noAuthNoPriv 1.3.6.1.6.3.10.2.1.1.0 For this reason, the engine ID must be recorded along with the device in your Configuration Management Database (CMDB) prior to generating localized keys since the process used to derive these keys is dependent upon the engine ID (see RFC 3414 section 2.6). In the event that an engine ID has been modified due to LPAR cloning or SNMPD.BOOTS file corruption on z/OS, then it will invalidate all previously generated User-based Security Model (USM) keys. These must be recreated by executing pwtokey against the new engine ID value. The steps to recreate keys are as follows: (1) Identify the new engine ID from either D ICSF,STATUS, or SNMPD.BOOTS; (2) execute pwtokey -p HMAC-SHA -u auth for each of the defined USM users; (3) modify SNMPD.CONF to include the new hexadecimal string representations of the localized keys; (4) perform a warm restart of OSNMPD; and (5) update the credential records within your NMS for both the authentication and privacy keys. Track your engine IDs in your configuration management database just as you would track IP addresses.

The reality is SNMPv3 migrations almost never fail on a technical level. What causes trouble are all the things that have to be in place before they start or can happen after they start. The seven problems in Table 5, as well as the key to their successful execution in a financial mainframe migration, lie in these environmental preconditions. [21], [22].

SNMPv3 represents a structural defense against an internal (insider) threat as it does not provide an insider threat capability as does SNMPv2c. Anybody who knows the SNMPv2c community string will have full SNMP access to all devices they are allowed to view, without the ability to be held accountable individually; e.g., every poll, set, etc., can be attributed to the community string only and NOT to a particular user. In SNMPv2c an attacker can perform a full MIB tree query to gather ALL of the network topology information from a managed device(s), modify device configurations, and/or steal network topology information without ANY type of audit trail being generated to link these actions back to the actual user performing them. The SNMPv3 user-based security model provides per-user credentials with localized keys, such that each SNMP operation performed by the user is cryptographically bound to a specific username.

Table 5: Implementation Challenges and Recommended Mitigations

Challenge	Root Cause	Recommended Mitigation
engineID mismatch on z/OS	SNMPD.BOOTS file corruption or LPAR cloning changes engineID, invalidating localized keys	Store engineID from SNMPD.BOOTS in configuration management; regenerate keys after any engineID change
AES not available on z/OS	ICSF is not active or CEX hardware is not configured	Activate ICSF SSDD; verify with D ICSF,STATUS; fall back to DES only as temporary measure
NMS SNMPv3 trap reception failure	SNMPv3 traps bind to the sending agent engine ID; NMS needs createUser entry per source	Pre-configure NMS with all source engine IDs; use INFORM PDUs (acknowledged) instead of TRAPs
Legacy devices without SNMPv3 support	Firmware too old; hardware end-of-life.	Segment legacy devices in isolated management VLAN with strict ACLs; schedule decommission
Administrator training overhead	SNMPv3 configuration requires understanding of USM, VACM, key localization, and engine IDs	Produce internal runbooks with copy-paste configuration templates; conduct lab exercises before production rollout
RACF SERVAUTH violations on OSNMPD	Subagent DPI connections require SERVAUTH class profiles not present in default RACF configuration	Define EZB.SNMPAGENT.sysname.tcpprocname profiles in SERVAUTH class; permit OSNMPD userid
SolarWinds node re-discovery	Changing SNMP version resets some performance baseline counters	Export baseline data before cutover; use Orion SDK to update credentials without deleting the node

The View-Based Access Control Model (VACM) then limits the amount of the MIB subtree that a given user has access to based upon their role within the organization; i.e., a monitoring operator would not be able to issue any set operations, and there could be a separate audit trail generated when using a break-glass account. When combined with the RACF SERVAUTH enforcement capabilities provided by IBM's z/OS operating system, each SNMP session would be attributable to a specific user ID, thereby providing individual accountability, which meets both requirements of NIST SP 800-53 Control IA-2 and PCI-DSS Requirement 8.2.1. Therefore, this per-user least-privileged access model is the primary structural defense mechanism against insider-initiated SNMP abuse in financial mainframe environments.

9. Compliance Framework Alignment

Table 6: Compliance Control Mapping for SNMPv3 Migration

Framework	Control	Requirement	SNMPv3 Satisfaction
PCI-DSS v4.0	2.2.7	All non-console admin access must use strong cryptography	authPriv with AES-128 satisfies strong cryptography requirements.
PCI-DSS v4.0	2.2	No default passwords or community strings	Community strings eliminated; USM has no defaults
PCI-DSS v4.0	8.2.1	Unique user IDs for all access	USM per-user credentials replace shared community
NIST 800-53 Rev.5	SC-8	Transmission confidentiality and integrity	HMAC-SHA-96 provides integrity; AES-128 provides confidentiality
NIST 800-53 Rev.5	IA-2	Individual identification and authentication	Per-user USM credentials with individual accountability
NIST 800-53 Rev.5	AC-3	Access enforcement	VACM enforces least-privilege MIB view access per user
NIST 800-53 Rev.5	CM-7	Least functionality; disable insecure protocols	SNMPv1/v2c disabled; SNMPv3 only enforced
NSA/CISA TA17-156A	Section 3	Use only SNMPv3 with authPriv; ACL restrict to NMS IPs	Full compliance: SNMPv3 authPriv + ACL on all devices
CIS IOS Benchmark [23]	Sec. 1.5	SNMP ACLs; encrypted passwords; no default communities	IP ACL on all SNMP groups/users; SHA passwords; communities removed [23]

10. Resource and Timeline Estimates

Table 7: Migration Task Resource Estimates (150 to 300-Device Environment)

Task	Person-Hours	Calendar Time	Key Dependencies
Asset discovery and inventory	24 to 40	1 to 2 weeks	Network access; NMS query permissions
VACM view design and credential schema	16 to 24	1 week	RACF engineering; NMS admin; security architect
Pilot deployment and validation	20 to 32	1 to 2 weeks	5-10 representative devices; change window
Configuration automation scripting	32 to 48	1 to 2 weeks	Python/Ansible; device reachability; lab environment
Phased rollout (150-300 devices)	80 to 120	3 to 4 weeks	Change management; maintenance windows
NMS reconfiguration (SolarWinds/Zabbix)	16 to 24	1 week	Parallel with device rollout
Cutover and legacy removal	12 to 20	3 to 5 days	Rollback plan: monitoring continuity confirmed
Post-migration validation and documentation	16 to 24	1 week	Compliance evidence package; runbook finalization
TOTAL (excluding ongoing hardening)	216 to 332	9 to 11 weeks	

11. Repeatable Playbook and Verification Checklist

The checklist in Table 8 encapsulates the complete migration verification sequence. Each item maps to a specific phase and can be independently audited as

evidence for PCI-DSS and NIST compliance assessments. Teams should use this checklist as a gate between phases: no phase advances until all preceding items are checked.

Table 8: SNMPv2-to-SNMPv3 Migration Verification Checklist

#	Verification Item	Phase	Compliance Ref.
1	All SNMP-enabled assets documented with version, community strings, and NMS associations	Discovery	PCI 2.2
2	Legacy devices without SNMPv3 support identified and firmware upgrade scheduled	Discovery	CM-7
3	VACM views restrict monitoring users to required MIB subtrees only	Design	AC-3, CISA TA17-156A
4	ACLs defined restricting SNMP access to authorized NMS IP addresses only	Design	CISA TA17-156A
5	z/OS ICSF active and AES-128 confirmed available via D ICSF,STATUS	Design	RFC 3826
6	NMS v2c and v3 polling values compared; no metric discrepancies for 48 hours	Pilot	All
7	USM_USER entries with localized SHA + AES keys added to z/OS SNMPD.CONF for all users	Config	RFC 3414
8	RACF SERVAUTH profiles created for subagent DPI connections	Config	IBM SC27-3650
9	Legacy community strings removed from all devices	Cutover	PCI 2.2.7, NSA
10	All NMS dashboards confirm data continuity without gaps post-cutover	Cutover	All
11	nmap UDP 161 scan confirms SNMPv1/v2c responses no longer returned	Validation	PCI 2.2.7
12	Compliance evidence package prepared (configs, scan output, NMS screenshots)	Validation	PCI, NIST

12. Forward-Looking Considerations: Modern Telemetry

SNMPv3 is the mandatory remedy, especially for the existing fleet of financial mainframe systems. The telemetry landscape is changing, with gNMI [24] (streaming over Protocol Buffers/HTTP/2 with mandatory TLS) and NETCONF [25] (SSH-encrypted YANG-modeled configuration) [26] becoming more popular. Neither IBM z/OS Systems nor IBM Network Switch and Gateway Services presently understands gNMI or either NETCONF or RESTCONF. SNMP remains the only supported way to monitor your devices. The OpenTelemetry API, which IBM is implementing gradually via the Z APM Connect product, points in the right direction for network observability. Practical action in the financial-mainframe ecosystem is hybrid SNMPv3 for z/OS and OpenTelemetry for everything else, with the comforting notion that SNMP in the z/OS world is unlikely to go away anytime in the next decade.

This paper specifically aligns its migration strategy with NSA/CISA critical infrastructure guidelines. Both the December 2024 CISA Enhanced Visibility and Hardening Guidance [11] and the NSA Network Infrastructure Security Guide [3] require SNMPv3 be used by all critical infrastructure sectors. Since financial mainframes are classified as critical infrastructure under CISA's Financial Services Sector designation, the above guidance applies directly and therefore is an acceptable position to defend against regulatory examination and incident investigation inquiries. The five-stage migration process and VACM least privilege configuration described in Section 7, combined with the ACL-restricted MGMT plane and Engine ID lifecycle control described in Section 8, provide network hardening that meets or exceeds the guidelines contained in both the CISA and NSA documents.

13. Limitations and Future Work

13.1. Limitations

The FAIR [13] risk reduction figures are based upon the assumptions below for Threat Event Frequency, Vulnerability, Exposure Factors, and Asset Value. These assumptions use a mid-sized financial institution having 150-300 SNMP-enabled devices as a base case. Note that the absolute reduction figures derived from this case study will differ between financial institutions of a different size. Nonetheless, the model suggests that a 90-96% reduction can be expected regardless of the size of the institution under consideration. There is no post-migration actual data available for specific migration projects.

The procedures to migrate from IBM z/OS 2.5 and Cisco IOS-XE are described in full detail. Migration from other vendors, such as Junos OS from Juniper, EOS on Arista switches, F5 BIG-IP load balancers, and storage

controllers, is touched on at the surface. It is still a requirement to remedy engine-level parser vulnerabilities such as CVE-2017-6742 [7] and CVE-2025-20352 [27], affecting both SNMPv2c and SNMPv3 modules. HMAC-SHA-96 per RFC 3414 is the specified baseline because HMAC-SHA-2 variants defined in RFC 7860 are not generally supported on z/OS or Cisco IOS-XE trains. This paper does not include measurements for the processor, memory, and communication overhead of using SNMPv3 in an LPAR on z/OS.

13.2. Future Work

SNMPv3 testing also would be beneficial for vendors such as Juniper, Arista, F5, and various storage controller vendors. As SNMPv3 and network devices more widely support stronger authenticator algorithms, such as HMAC-256 recommended in RFC 7860, their adoption becomes viable. Architecture designs that employ hybrid data collection schemes between SNMPv3 collection from mainframe z/OS devices and the gNMI [24], NETCONF [25], and SNMPv3-supported OpenTelemetry provide additional architectural guidance to designers. In the same spirit as the previous statement, there also exist automation software such as Ansible and tools such as pyATS that significantly reduce the effort required to operate, validate, and roll back during the migration of large heterogeneous SNMP fleet systems, which require only a few percent of the person-hour figures previously reported in Table 7 to perform such large migration projects. Longitudinal observational studies on network systems affected by such upgrades or rollbacks also can provide additional useful information to designers.

Empirical benchmarks of SNMPv3 authPriv CPU and memory usage should be conducted on z/OS LPARs that use ICSF hardware-accelerated crypto rather than software-only crypto to create the type of quantitative information that architects require when deciding which LPAR resource allocations will meet their needs after migrating their current systems. In addition to validating the results of the benchmarks, these tests would also serve as a testbed to determine if the high CPU utilization noted in the Limitations section can be mitigated solely through the use of hardware cryptography or if some reduction in polling frequency will still be required. If an organization chooses to leverage configuration management automation (such as Ansible) with either IBM z/OS-compatible modules or PyATS for Cisco IOS-XE validation, they will potentially reduce the amount of time spent on each device by 60-80%, as indicated in the 3rd row of Table 7, for example.

AI-based anomaly detection can be applied to SNMPv3 traps and inform and alert an administrator whenever there is anomalous behavior detected (e.g., an unauthorized polling attempt or a sudden change in engine ID or a violation of VACM policies). This method provides an advantage over traditional static SIEM correlation rules because it has the capability to detect anomalies as they occur in near-real-time, whereas static SIEM correlation rules rely upon historical knowledge. Automating Configuration Deployment and Using AI-Assisted Post-Migration Monitoring represent the natural next iteration of the Repeatable Playbook described above. To better understand how to scale the SNMPv3 management plane to accommodate cloud-resident network devices and containerized workloads, the scalability of SNMPv3 to accommodate hybrid cloud models requires further research.

14. Conclusion

This paper has demonstrated that SNMPv2c is fundamentally flawed as a mechanism for remotely managing financially critical mainframes. It has also demonstrated that a fully qualified path to securely remotely access such systems exists, is proven to work in production, and is in the economic reach of even the most fiscally lean enterprise. To address these flaws, SNMPv3 provides security using the User-based Security Model, defined by RFC 3414. Instead of using a simple community string for plaintext communication, SNMPv3 provides cryptographic authentication of host identity via HMAC-SHA-96 and optional confidential communication via AES-128 CFB. The SNMP view-based access control model defined in RFC 3415 enables granular, auditable control over SNMP access.

The FAIR-based risk analysis establishes that migration reduces expected annual loss from the $1.1M to $4.5M range under SNMPv2c to $40,000 to $250,000 under SNMPv3 authPriv, a reduction of 90 to 96 percent. This calculation does not include compliance penalty avoidance or reputation protection value, making the actual benefit larger. The migration investment of $50,000 to $200,000 and nine to eleven weeks of elapsed time is recovered within one to three months of post-migration operation.

The five-phase methodology presented here, from structured inventory through parallel-run validation and legacy removal, generalizes to any organization operating SNMP-managed infrastructure. The parallel coexistence capability of both z/OS SNMPD.CONF and Cisco IOS eliminates the primary operational risk of migration. The 12-item verification checklist provides an independent, audit-ready evidence record. For security architects and mainframe operations teams, the conclusion is unambiguous: SNMPv2c should be disabled immediately, and SNMPv3 with authPriv, SHA, AES-128, and ACL-restricted access to authorized NMS hosts should be the only SNMP version operating on financial mainframe infrastructure.

Funding

This research received no external funding.

Author Contributions

Rohit Kumar Shaw is the sole author and conducted all aspects of this research, including conceptualization, methodology, analysis, and writing.

Conflicts of Interest

The author declares no conflict of interest.

References

[1] J. Case, R. Mundy, D. Partain, and B. Stewart, "Introduction and Applicability Statements for Internet-Standard Management Framework," IETF RFC 3410, Dec. 2002, doi: https://doi.org/10.17487/RFC3410.

[2] Cybersecurity and Infrastructure Security Agency, "Reducing the Risk of SNMP Abuse," Alert TA17-156A, Jun. 5, 2017. [Online]. Available: https://www.cisa.gov/news-events/alerts/2017/06/05/reducing-risk-snmp-abuse

[3] National Security Agency, "Network Infrastructure Security Guide," Cybersecurity Technical Report U/OO/118623-22, ver. 1.2, Oct. 2023. [Online]. Available: https://media.defense.gov

[4] D. Harrington, R. Presuhn, and B. Wijnen, "An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks," IETF RFC 3411, Dec. 2002, doi: https://doi.org/10.17487/RFC3411.

[5] U. Blumenthal and B. Wijnen, "User-based Security Model (USM) for Version 3 of the Simple Network Management Protocol (SNMPv3)," IETF RFC 3414, Dec. 2002, doi: https://doi.org/10.17487/RFC3414.

[6] B. Wijnen, R. Presuhn, and K. McCloghrie, "View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)," IETF RFC 3415, Dec. 2002, doi: https://doi.org/10.17487/RFC3415.

[7] National Vulnerability Database, "CVE-2017-6742 Detail: Cisco IOS SNMP Buffer Overflow," 2017. [Online]. Available: https://nvd.nist.gov/vuln/detail/CVE-2017-6742

[8] National Cyber Security Centre, National Security Agency, Cybersecurity and Infrastructure Security Agency, and Federal Bureau of Investigation, "APT28 Exploits Known Vulnerability to Carry Out Reconnaissance and Deploy Malware on Cisco Routers," Joint Advisory, Apr. 2023. [Online]. Available: https://www.ncsc.gov.uk

[9] U. Blumenthal, F. Maino, and K. McCloghrie, "The Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP User-based Security Model," IETF RFC 3826, Jun. 2004, doi: https://doi.org/10.17487/RFC3826.

[10] N. Lawrence and P. Traynor, "Under New Management: Practical Attacks on SNMPv3," in Proc. 6th USENIX Workshop on Offensive Technologies (WOOT), Bellevue, WA, USA, Aug. 2012, doi: https://doi.org/10.5555/2372399.2372416.

[11] Cybersecurity and Infrastructure Security Agency, "Enhanced Visibility and Hardening Guidance for Communications Infrastructure," Dec. 2024. [Online]. Available: https://www.cisa.gov

[12] Cisco Systems, "Cisco IOS and IOS XE Software SNMP Denial of Service and Remote Code Execution Vulnerability," Security Advisory cisco-sa-snmp-x4LPhte, Sep. 24, 2025. [Online]. Available: https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snmp-x4LPhte

[13] J. Freund and J. Jones, Measuring and Managing Information Risk: A FAIR Approach. Waltham, MA, USA: Butterworth-Heinemann, 2014.

[14] PCI Security Standards Council, "Payment Card Industry Data Security Standard: Requirements and Testing Procedures, Version 4.0," Mar. 2022. [Online]. Available: https://www.pcisecuritystandards.org

[15] Joint Task Force, "Security and Privacy Controls for Information Systems and Organizations," National Institute of Standards and Technology, Gaithersburg, MD, USA, NIST Special Publication 800-53 Rev. 5, Sep. 2020, doi: https://doi.org/10.6028/NIST.SP.800-53r5.

[16] J. Schönwälder, A. Pras, M. Harvan, J. Schippers, and R. van de Meent, "SNMP Traffic Analysis: Approaches, Tools, and First Results," in Proc. 10th IFIP/IEEE Int. Symp. Integrated Network Management (IM), Munich, Germany, May 2007, pp. 323–332, doi: https://doi.org/10.1109/INM.2007.374797.

[17] IBM, "USM_USER Entry," IBM z/OS V2.5.0 Documentation. [Online]. Available: https://www.ibm.com/docs/en/zos/2.5.0

[18] IBM, "SNMPD.CONF Sample," IBM z/OS V2.5.0 Documentation. [Online]. Available: https://www.ibm.com/docs/en/zos/2.5.0

[19] Cisco Systems, "Configuration Template for SNMPv3," Cisco Community Knowledge Base, Document ID 4666450. [Online]. Available: https://community.cisco.com

[20] Cisco Systems, "Disable SNMPv1 or SNMPv2c While Other Versions Remain Enabled," Document ID 113469. [Online]. Available: https://www.cisco.com

[21] L. Andrey, O. Festor, A. Lahmadi, A. Pras, and J. Schönwälder, "Survey of SNMP Performance Analysis Studies," International Journal of Network Management, vol. 19, no. 6, pp. 527–548, Nov. 2009, doi: https://doi.org/10.1002/nem.729.

[22] S. Kuryla and J. Schönwälder, "Evaluation of the Resource Requirements of SNMP Agents on Constrained Devices," in Managing the Dynamics of Networks and Services, Lecture Notes in Computer Science, vol. 6734. Berlin, Germany: Springer, 2011, pp. 100–111, doi: https://doi.org/10.1007/978-3-642-21484-4_13.

[23] Center for Internet Security, "CIS Cisco IOS Benchmark," ver. 2.2, 2023. [Online]. Available: https://www.cisecurity.org

[24] OpenConfig, "gNMI Specification," ver. 0.10.0, GitHub, 2023. [Online]. Available: https://github.com/openconfig/gnmi

[25] R. Enns, M. Björklund, J. Schönwälder, and A. Bierman, "Network Configuration Protocol (NETCONF)," IETF RFC 6241, Jun. 2011, doi: https://doi.org/10.17487/RFC6241.

[26] F. K. Ariefputra and E. Mulyana, "Performance Analysis of gNMI Streaming Telemetry-Based Monitoring Systems Using Containerlab Network Simulation," Jurnal Nasional Teknik Elektro dan Teknologi Informasi, vol. 13, no. 2, pp. 101–107, 2024, doi: https://doi.org/10.22146/jnteti.v13i2.10185.

[27] National Vulnerability Database, "CVE-2025-68615 Detail: Net-SNMP snmptrapd Buffer Overflow," 2025. [Online]. Available: https://nvd.nist.gov/vuln/detail/CVE-2025-68615

Copyright: This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY-SA) license (https://creativecommons.org/licenses/by-sa/4.0/).

Rohit Kumar Shaw is an Infrastructure Engineer specializing in mainframe infrastructure and network security with deep expertise in IBM z/OS, z/VM, SNMP, AT-TLS, RACF and ACF2, NetView, Omegamon, Splunk, and z/OSMF. He holds a degree in Computer Science and has worked across disaster recovery testing, certificate renewals, SNMPv2-to-SNMPv3 hardening, AT-TLS policy

deployment, TCP/IP configuration standardization, and platform modernization in financial services environments. His current research interests include zero-trust transport security on legacy mainframes, SSH compliance automation under z/OS USS, RAG-based retrieval for enterprise operations, and Kerberos versus public key authentication patterns. He has written extensively on these topics for IEEE-format research papers and trade publications, with a focus on producing publication-ready guidance for security architects and mainframe operations teams.