Revista Multidisciplinar do Nordeste Mineiro, v.12, 2025
ISSN 2178-6925
DOI: 10.61164/rmnm.v12i1.4231

ANÁLISE E MAPEAMENTO DE ERROS DE LOG NO ACTIVE DIRECTORY EM AMBIENTE DE PRODUÇÃO REAL: UM ESTUDO DE CASO NA EMPRESA USINAS ITAMARATI (UISA)

ANALYSIS AND MAPPING OF LOG ERRORS IN ACTIVE DIRECTORY IN A REAL PRODUCTION ENVIRONMENT: A CASE STUDY IN COMPANY USINAS ITAMARATI (UISA)

Raul Gonçalves Muller
Bachelor in Computer Science, Mato Grosso State University, Brazil
E-mail: raul.goncalves.muller@unemat.br
ORCID: https://orcid.org/0009-0008-2156-7109

Raquel da Silva Vieira Coelho
Master of Computer Science, Mato Grosso State University, Brazil
E-mail: raquelcoelho@unemat.br
ORCID: https://orcid.org/0009-0004-0407-096X

Diógenes Antonio Marques José
Master of Computer Science, Mato Grosso State University, Brazil
E-mail: dioxfile@unemat.br
ORCID: https://orcid.org/0000-0002-9707-6022

Recebido: 15/06/2025 – Aceito: 26/06/2025

Resumo

Em redes corporativas, o ***Active Directory (AD)*** é uma das principais ferramentas para gerenciar, centralizar e autenticar o acesso de usuários e serviços. Nesse contexto, mapear os principais erros relacionados ao AD é fundamental para prevenir falhas futuras. Este artigo apresenta um estudo de caso realizado na Empresa Usinas Itamarati (UISA), que conta com 4.000 usuários no AD, com base na análise de logs coletados entre janeiro de 2022 e dezembro de 2023. Assim, foram identificados os 10 erros mais frequentes, classificados em duas categorias: **Logs de Aplicativos** e **Logs de Sistema**. Cada erro foi mapeado, categorizado e representado por gráficos e tabelas, considerando tipo, classe, frequência, perfil do usuário afetado e possíveis soluções. Os resultados demonstram que a sistematização dos erros contribuiu significativamente para a identificação de falhas recorrentes, avaliação de impactos no ambiente corporativo e desenvolvimento de soluções práticas e eficazes.

Palavras-chave: Microsoft Windows; Active Directory; Logs de eventos; Ambiente corporativo.

Abstract

In corporate networks, Active Directory (AD) is one of the main tools for managing, centralizing, and authenticating user and service access. In this context, mapping the main errors related to AD is essential to prevent future failures. This article presents a case study at Usinas Itamarati (UISA) Company, which has 4,000 users in AD, based on the analysis of logs collected between January

2022 and December 2023. Thus, the 10 most frequent errors were identified and classified into two categories: Application Logs and System Logs. Each error was mapped, categorized, and represented by graphs and tables, considering type, class, frequency, affected user profile, and possible solutions. The results demonstrate that the systematization of errors contributed significantly to identifying recurring failures, assessing impacts on the corporate environment, and developing practical and effective solutions.

Keywords: Microsoft Windows; Active Directory; Event logs; Corporate environment.

1. Introduction

Active Directory (AD) is a core component of the ***Microsoft Windows*** operating system, widely adopted in corporate environments for managing user access and network resources. It consists of a set of files stored on the domain server, responsible for recording and controlling usernames and passwords, file and printer access permissions, disk quotas, user activity times, and other key configurations **(Controle Net, 2022)**. Given the central role AD plays in ensuring secure, efficient access to computing resources and corporate networks, it becomes essential to investigate the main errors and failures that affect its operation. In organizational settings — where time efficiency and information security are critical — identifying, categorizing, and quantifying these errors is vital for maintaining operational continuity and minimizing risks.

Thus, this study is particularly motivated by the limited availability of comprehensive research in the literature that addresses AD errors from a broad operational perspective. For instance, **Benjamin et al. (2024)** explore the use of AD logs for training artificial intelligence models, but do not detail the classification of events by type or origin. Similarly, **Basem et al. (2022)** provide a step-by-step analysis of AD attacks focused on the ***Kerberos*** authentication protocol, though their investigation is confined to that specific context. **Carlos et al. (2021)** employ event logs for continuous monitoring of Kerberos-related threats, yet limit their scope to attack-related data. **Thomas and Hisham (2022)** offer valuable insights into AD log event codes and expected behaviors under normal conditions, but their work also concentrates exclusively on potential security breaches. Moreover, all of these studies were conducted in virtualized environments, which may not fully represent the behavior and challenges encountered in real-world production systems. In contrast, this research proposes a more comprehensive approach by analyzing a wide range of AD errors — extending beyond security issues to include network, application, and configuration-related failures. To support AD administrators in promptly identifying and resolving such issues, this study developed a taxonomy of error types along with their corresponding solutions. The research is structured as a case study conducted in a real production environment at Usinas Itamarati (UISA) Company, which comprises 4,000 AD users — 2,500 employees and 1,500 devices. The analysis was carried out over a two-year period, from **January 2022 to December 2023**, using logs generated by ***Active Directory 2016*** on ***Windows Server 2019***. Throughout the study, all recorded errors were systematically mapped and categorized. These were then presented through graphs and tables, enabling analysis of the following parameters: i) Type and class of each error; ii) Frequency of occurrence; iii) Profile of users generating and/or detecting the error; iv) Potential solutions for each error.

The results demonstrated that structured error mapping significantly enhanced the ability to identify recurring issues, evaluate their impact on the corporate environment, and develop effective, targeted solutions. Furthermore, the study helped profile the users most frequently involved in generating or identifying the most critical errors, providing additional insight into preventive measures.

The remainder of this paper is organized as follows: in **Section 2** outlines the theoretical background; **Section 3** describes the proposed methodology; **Section 4** discusses related work; **Section 5** presents the results and analysis; and finally, **Section 6** concludes the study and suggests directions for future research.

2. Theoretical Basis

This section presents the main concepts related to Active Directory (AD). In other words, to understand the function of AD, it is necessary to know which services and entities AD manages.

2.1 Network Security

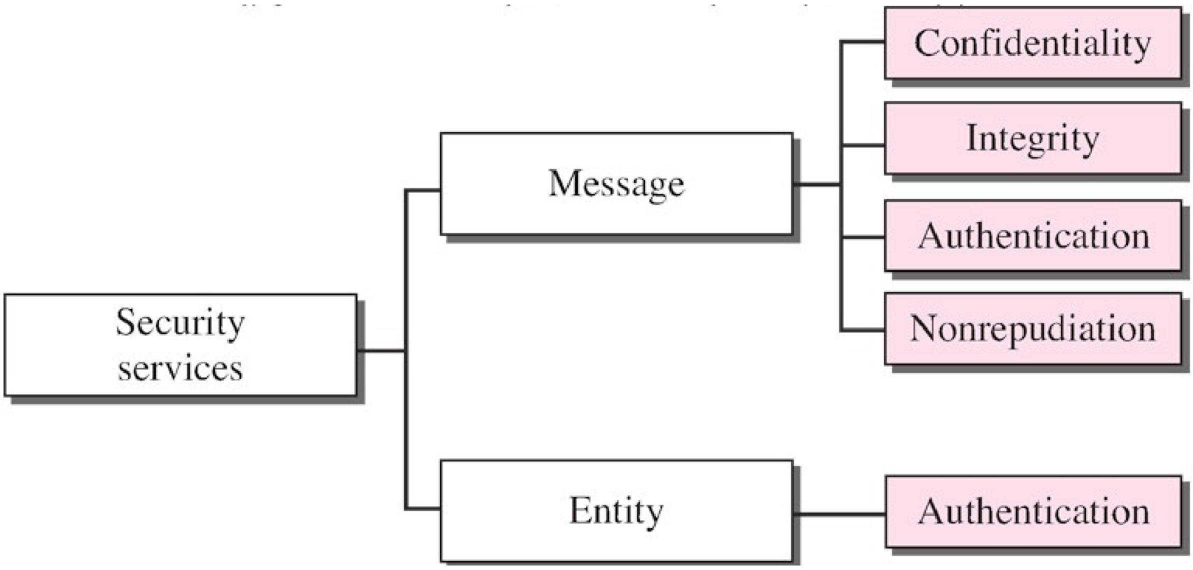
The concept of network security permeates the basis of Internet cyber protection. Therefore, it is an important topic for this research because AD helps in this context. Thus, this topic is intrinsically linked to AD.

For **Moraes (2010, p. 16)**, a system is secure if and only if it behaves the way you expect it to. Therefore, network security can be defined as an act of defending against malicious usurpation of information, whether unforeseen or intentional, by people inside or outside the system, including clients, administrators, or attackers. As discussed by **Barreto, Zanin, and Saraiva (2018, p. 11)**, network security must ensure that all messages exchanged within a network are sent to the final recipient, without any changes along the way.

2.1.1 Network Security Services

Network security services comprise three characteristics: confidentiality; integrity; and availability. In addition to these fundamentals, there are other security characteristics such as non-repudiation, authentication, authorization, and auditing **(Moraes, 2015, p. 20)**. From the point of view of network security services, these services aim to prevent attacks on the network and all assets connected to it **(Barreto, Zanin, and Saraiva, 2018, p. 13)**.

Figure 1 – Message or Entity-Related Security Services.



Source: (Forouzan, 2010).

2.1.2 Domain Name System

DNS is an important network service that must be protected by network security. For **Moraes (2010, p. 154)**, a Domain Name System (DNS) is the mechanism in which Internet domain names are located and translated into IP addresses. For example, it is easier to remember the domain name than the IP address. Another definition can be found in Kurose and Ross (2021, p. 99), for example, it is the ability to translate names into numbers or vice versa.

2.1.3 Firewall

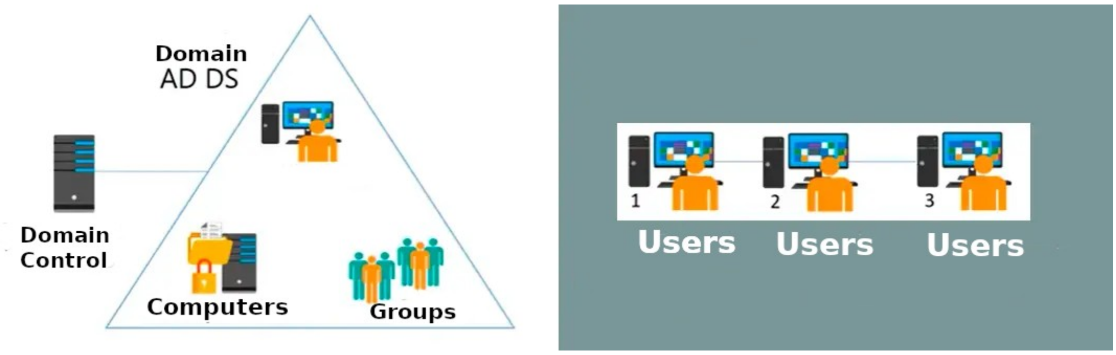
A firewall serves as a fundamental component of internet security, functioning as a combination of hardware and software designed to segregate internal network traffic from external internet traffic. Its primary role is to control the flow of data packets by authorizing or blocking their passage based on predefined rules **(Kurose & Ross, 2021, p. 537)**. Additionally, firewalls act as traffic filters, configurable by network administrators to permit or deny specific types of connections **(Barreto, Zanin, & Saraiva, 2018, p. 14)**.

According to **Kurose and Ross (2021, p. 538)**, firewalls can be categorized into three main types: traditional packet filters, stateful filters, and application gateways. Traditional packet filters operate by examining socket addresses — combinations of IP addresses and port numbers (e.g., ***192.178.9.1:80***) — to determine whether to allow or block a packet. Stateful filters, on the other hand, maintain awareness of active TCP connections and use this contextual information to make more informed filtering decisions. Lastly, application gateways function as dedicated proxy servers, requiring all inbound and outbound traffic to pass through them for inspection and control **(Kurose & Ross, 2021, p. 541)**.

2.2 Active Directory

Active Directory is a Microsoft directory service that was pre-launched around the 1990s and was consolidated in the market from 2000 onwards with Windows 2000. In this context, it arose from the need to have a single directory that allowed the user to access it through a single password. AD manages access to directories (e.g., shares, storage units, printers, etc.), network services, and applications by authenticating users and devices **(Net Control, 2022)**.

Figure 2 – AS DS Domain and Working Groups.



Source: (Controle Net, 2022).

In addition, AD stores information about objects on the network and makes this information easy to find and use by administrators and users. Furthermore, AD uses a structured data store as the basis for a logical and hierarchical organization of directory information **(Foulds et al., 2023)**.

2.2.1 Active Directory Specifications

As discussed in **Foulds et al. (2023)**, security is integrated into AD through logon authentication and access control to objects in the directory. With a single network logon, administrators can manage directory and organization data across the network, and authorized network users can access resources anywhere on the network. In this way, policy-based administration facilitates the management of more complex networks. Thus, for AD to ensure the security and control of the environment, the following processes are carried out: **(i)** authentication, such as user credentials and password; **(ii)** authorization, making visible only data and services to which they have permission; **(iii)** name resolution, enabling the location and communication of clients via DNS; **(iv)** centralized management, defining the control of a vast diversity of organizations in a single place, all behind a resource tool called Group Policy **(Controle Net, 2022)**.

In addition, AD also has a set of “Schema” rules containing all defined objects stored in a directory, their restrictions and limits on the objects themselves, and the format of their names. Among other things, it has a global catalog, with the data of each object in the directory, allowing the sharing of information from this directory for users and administrators, regardless of which directory the information resides in. In addition, AD has a query and index mechanism, so that objects and their respective properties can be informed and searched for by applications or users on the network. Finally, there is the replication service, which distributes the data from its directories across a network. In this context, all domain controllers perform this replication and contain a complete copy of all the data from the directories in their respective domains. Consequently, any changes to the data are replicated across all domain controllers **(FOULDS et al., 2023)**.

3. Proposal Description

The scope of this work is focused on the analysis of Active Directory logs in a corporate production environment belonging to Usinas Itamarati (UISA) Company, which recently underwent an organizational restructuring process. Thus, to map the events recorded in the logs, a survey was conducted on related work that served as a basis for classifying the occurrences according to their level of criticality and for proposing appropriate corrective solutions.

3.1 Methodology

This section presents the methodological procedures used to map the most frequent errors that occur in the **AD directory service**. To this end, a survey was carried out of all error events in the AD LOG from 01/2022 to 12/2023 and on the servers of a real corporate environment called Company Usinas Itamarati (UISA). In this context, the aim was to identify the following parameters: **(a)** Type of Error and class to which the error belongs; **(b)** Frequency at which the error occurs; **(c)** Profile of the User who generates and/or identifies the error; and **(d)** Possible Solution to the Error.

Given the above, the ten most common errors in AD were the targets of this study. Thus, to carry out the data collection, exploratory research was used which, according to **Lakatos (2021, p. 24)**, is based on the principle that a chapter or section deals with a subject that may be of interest, but may omit the aspect directly related to the problem that is the object of the research. Furthermore, as described in Marconi and **Lakatos (2022, p. 295)**, this type of study allows greater familiarity with the problem and the construction of hypotheses.

Consequently, during the study, a **Case Study** was also used, which aimed to collect data on frequent AD errors and their impacts on user productivity. According to **Marconi and Lakatos (2022, p. 306)**, a **Case Study** is a review with greater depth of a defined case or group of people under all their characteristics.

However, it is limited because it is confined only to the case studied, which cannot be generalized. In addition, to present the related works, the research used the bibliographic review of the literature which, as discussed by **Lakatos (2021, p. 285)**, consists of a synthesis, as complete as possible, regarding the work and the data pertinent to the topic, within a logical sequence.

To compose the related works section, a systematic search was conducted using three academic research platforms: **Google Scholar**, the **CAPES Journal Portal**, and **IEEE Xplore**. The following search queries were applied:

1. **Google Scholar**: "Active Directory" event analysis;
2. **CAPES Journal Portal**: "Active Directory" AND event AND analysis;
3. **IEEE Xplore**: ("All Metadata":Active Directory) AND ("All Metadata":event) AND ("All Metadata":analysis).

The selection criteria focused on works published between **2020 and 2025** that were directly relevant to the research topic.

On **Google Scholar**, the first 100 results were reviewed based on their titles, from which **20** were shortlisted. These were then filtered by reading their abstracts, resulting in **7** relevant studies. A final, in-depth review narrowed the selection to **4 works** that were included in the literature review.

In the **CAPES Journal Portal**, only **one relevant publication** was identified and selected after analysis. The **IEEE Xplore** search returned **7 results**, of which **only one** met the criteria for inclusion.

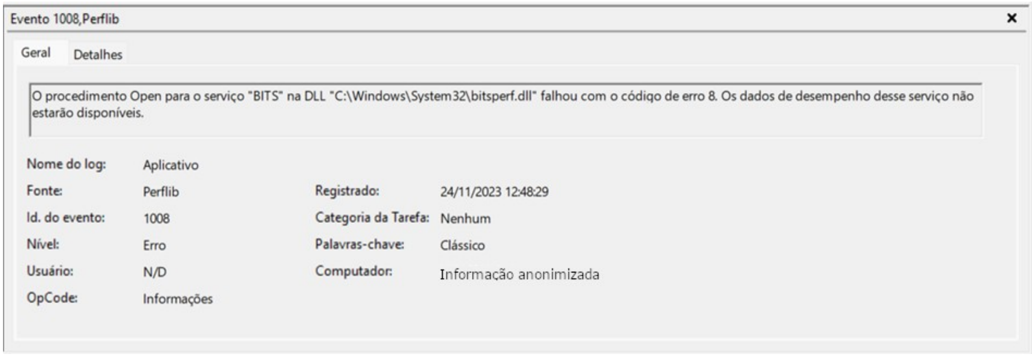
3.2 Log Categorization in Alpha Company

This section describes the process used to catalog Active Directory (AD) error logs. The logs were organized into two main categories: **System Logs** and

Application Logs. A date filter was applied to collect entries within the period from **January 1, 2022, at 00:00:00** to **December 31, 2023, at 23:59:59**.

To retrieve the data, the **Windows Event Viewer** was utilized, allowing access to all relevant log entries within the defined timeframe. The extracted information was then exported to a **.csv file** for further analysis. To process and visualize the data, a Python script was developed using the **pandas** and **matplotlib** libraries. This script was responsible for generating the graphs presented in the subsequent sections of this work. The complete source code is publicly available and can be accessed at the following repository: https://github.com/Ragomu/plot-event-ids.git. Therefore, based on this analysis, an **absolute count** of the error events generated by Active Directory (AD) was conducted. The logs were then **categorized** according to their type — primarily into **System Logs** and **Application Logs** — following the predefined classification criteria. **Figure 3** illustrates an example of an error found in the Application Logs, as viewed in the **Windows Event Viewer**, including general details such as the event description, source, timestamp, and the machine from which it originated. The following section presents an assessment of the **criticality levels** of the identified error events, ranging from **Level 5** (most disruptive) to **Level 1** (least impactful). Additionally, it discusses the **sources** of these errors and, where applicable, proposes **potential solutions**. It is important to note that while some errors may indicate underlying issues requiring remediation, others are expected behaviors within the designed operation of AD and do not necessarily represent faults.

Figure 3 – Example of an Error Log Event in the Windows Event Viewer.



O procedimento Open para o serviço "BITS" na DLL "C:\Windows\System32\bitsperf.dll" falhou com o código de erro 8. Os dados de desempenho desse serviço não estarão disponíveis.

Nome do log:	Aplicativo		
Fonte:	Perflib	Registrado:	24/11/2023 12:48:29
Id. do evento:	1008	Categoria da Tarefa:	Nenhum
Nível:	Erro	Palavras-chave:	Clássico
Usuário:	N/D	Computador:	Informação anonimizada
OpCode:	Informações		

Source: Author.

4. Related Work

This section presents a summary of the selected works, as described in Section 3. Table 1 presents the articles that were selected based on the bibliographic research carried out on the CAPES Journals, Google Scholar, and IEEE Xplorer portals.

Table 1 – Articles Selected for the Related Works Section.

Title	Log Event Level	Purpose of Analysis	Environment Type
Benjamin Keyogeg,et al,.2024	All Levels	Ransomware detection	Virtualized
Basem Ibrahim Mokhtar, et al., 2022	Information Level	Advanced Persistent Threat Detection	Virtualized
Carlos Díaz Motero, et al., 2021	Information Level	Threat Assessment	Virtualized
Thomas Grippo, Hisham A. Kholidy, 2022	Information Level	Threat Detection in the Kerberos Protocol	Virtualized
Weifeng Wang, et al., 2020	Information Level	Advanced Persistent Threat Detection	Simulated
Tarek Radah, Habiba Chaoui, Chaimae Saadi 2023	Information Level	Identifying malicious authentication patterns	Production
Raul Gonçalves Muller, Raquel da Silva Vieira Coelho, Diógenes Antônio Marques José, 2025	Error Level	Troubleshooting	Production

Source: Author.

In the work of **Benjamin et al. (2024)**, a search for events generated in the AD log is carried out using a machine-learning model based on random forests. The objective was to detect ransomware in environments with centralized network access in Windows Active Directory Domain Services (AD DS). According to the authors, the methods for detecting ransomware were focused on behavioral analysis, log aggregation, and dynamic monitoring. This detection system involved log events that allow a detailed view of how ransomware usually changes system settings to encrypt data and gain privileges. The experiments were carried out in a simulated environment through virtualization with VMware and Hyper-V. Consequently, AD services were adjusted to monitor domain activities and irregular login attempts. Therefore, an extensive collection of logs was carried out from all machines in the simulated AD environment. The tools used to collect the logs were: Sysmon, PowerShell, and the ELK Stack for real-time log accumulation and analysis. However, the logs are simply collected and aggregated, with no mention of classification, and only considered for their associations with ransomware activities, all in a virtualized environment.

Basem et al. (2022) present a detailed step-by-step analysis of attacks targeting Active Directory (AD), focusing specifically on the **Kerberos authentication flow**. The study outlines the various stages of these attacks, which are designed to escalate privileges within the domain environment. To this end, the researchers simulate and analyze two types of **advanced persistent threats (APTs)** with the objective of identifying corresponding indicators in **Windows event logs**. The experimental environment was built using **VMware Workstation 14**, hosting two virtual machines running **Windows Server 2016**. This setup enabled the execution of a variety of security tools, including: **Mimikatz 2.0**, for extracting Kerberos tickets used in multiple attack techniques; **PSEXEC**, for remote execution of Windows commands within the virtual network; **FileZilla Server**, serving as an FTP server in Kerberoasting and Hashcat-related attacks; **Powerview**, for domain enumeration and vulnerability reconnaissance to identify exploitable weaknesses for privilege escalation. Among the results, the study highlighted the detection of **"Pass-the-Hash"** behavior — a well-known technique used to elevate privileges without requiring plaintext passwords. The findings demonstrate how specific patterns in log events can be indicative of malicious activity, contributing to improved detection and response strategies for AD-based attacks.

Carlos et al. (2021) investigate the main attacks on Kerberos in Windows environments with AD. They point out the disadvantages that the system imposes, such as the centralization of authentication with a single point of failure, that is, all users must have their clocks synchronized and all access keys are stored on a central server. In addition, an experiment is presented in which a series of attacks are analyzed to acquire attack patterns and detect tools that can be used in the attack. In this context, the authors intended to quantify the difficulty of executing a given attack and the difficulties of detecting and mitigating attacks. Therefore, event logs were used as a method of continuous monitoring of these environments to detect these attacks.

The study conducted by **Thomas and Hisham (2022)** investigates the impact of **Golden Ticket** and **Silver Ticket** attacks on a **virtualized Active Directory (AD)** environment utilizing **Kerberos authentication**. For the simulation, a simplified domain controller infrastructure was established, consisting of a **Windows Server 2019** running AD, a **Windows 10 client**, and a **SQL Server**. The environment was virtualized using **VirtualBox** as the hypervisor. To detect these types of attacks, the researchers relied on the analysis of **Windows security event logs**. In the context of Kerberos authentication, several event codes are critical for monitoring suspicious activity, including **4624**, **4634**, **4672**, and **4769**. The first three codes are associated with **logon and logoff events**, while **event ID 4769** is directly related to the **Kerberos Ticket Granting Service (TGS)** — a key focus for detecting ticket-based attacks. The study highlights a significant anomaly: during suspected Golden or Silver Ticket attacks, **event 4769** often lacks essential details, such as the **client hostname**. This absence may indicate unauthorized ticket generation, especially when 4769 is not accompanied by expected logon events. Such discrepancies serve as potential indicators of malicious activity targeting AD's Kerberos authentication flow.

Weifeng et al. (2020) analyze the most common domain intrusion methods. Based on the analysis of log files generated during attacks, specific detection rules are defined and then integrated into an automated analysis mechanism. To this end, the work proposes the construction of a network framework used in the simulation of environments with domains. In this environment, the domain control server continuously generates event logs, which are collected by Winlogbeat and sent to Logstash for formatting. The data is then forwarded to RabbitMQ, which is responsible for storing the messages in a cache, enabling later processing.

In the study presented by **Tarek, Habiba, and Chaimae (2023)**, a method for detecting malicious activity within the **authentication process** is proposed, based on **statistical analysis** of log data. To validate the effectiveness of the approach, the authors conducted experiments in a **real corporate production environment**, where a series of **log events simulating malicious behavior** were deliberately generated. The goal was to demonstrate the method's capability to accurately identify **suspicious authentication attempts**. Although the testing took place in a live production setting, it is important to note that the events analyzed were **synthetic** — the result of **controlled simulations** — and did not originate from actual security incidents within the environment.

5. Results and Discussion

This section presents the cataloging of AD error logs in the production environment of Usinas Itamarati (UISA) company, as well as their summary to map the ten most frequent types of error logs in AD.

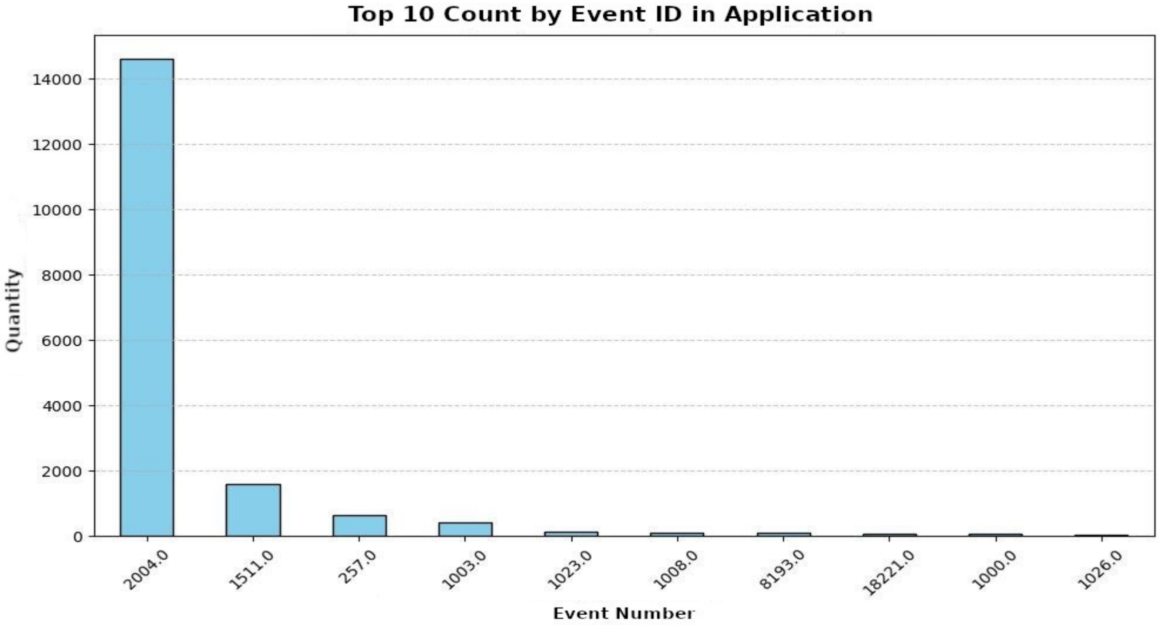
Consequently, we will present tables, Tables 1, 2, 3, and 4 with the ten most frequent errors and their possible solutions.

Furthermore, when performing this analysis, 17,381 errors were raised in the Application Errors Category while 565,903 error logs were raised in the System Errors Category, a difference of approximately 33 times more than the first mentioned. Another difference, also, is in the distribution of the frequency in which these errors occur.

Thus, the following sections will present and discuss the main peculiarities of this analysis, in addition to providing more details on the criticality, origin, and solutions of each of these events.

5.1 Application Log Data Collection

Figure 4 – Python Subplot Graph of Event Count in Application Log.



Source: Author.

As observed in **Figure 4**, the most frequent application error event is code 2004. This event has eight times more occurrences in the logs compared to event 1511, the second most frequent in the extracted data. Consequently, in a more detailed analysis, it was observed that error 2004 represents 82.00% of all errors in the analyzed period (e.g., 01/01/2022 00:00:00 to 12/31/2023). Furthermore, event 1511 is in 2nd place, with a frequency of 8.91% compared to the other error codes. In 3rd and 4th place are codes 257 and 1003, with the following occurrence frequencies of 3.54% and 2.26%, respectively.

Therefore, the other codes, added together, are below 1%. Regarding the nature of the error, code 2004 is a server monitoring error. In this context, this means that one of the servers does not have administrative access to access its information. The events originate from PerfNet, which monitors the performance of server services, counting several properties, for example: the number of times a domain announced itself to the network or the number of times servers in the same domain announced themselves to the server with the service being monitored. Regarding code 1511, this occurs when there are errors in accessing user files, which may have been corrupted or deleted. Therefore, regarding code 257, this means, for example, that the physical path of a partition was recovered (e.g., C: or D:), which may indicate that an error in the file system is being observed. The error descriptions can be seen in **Table 2**. In addition, more details about the error codes can be seen in **Subsection 5.3**.

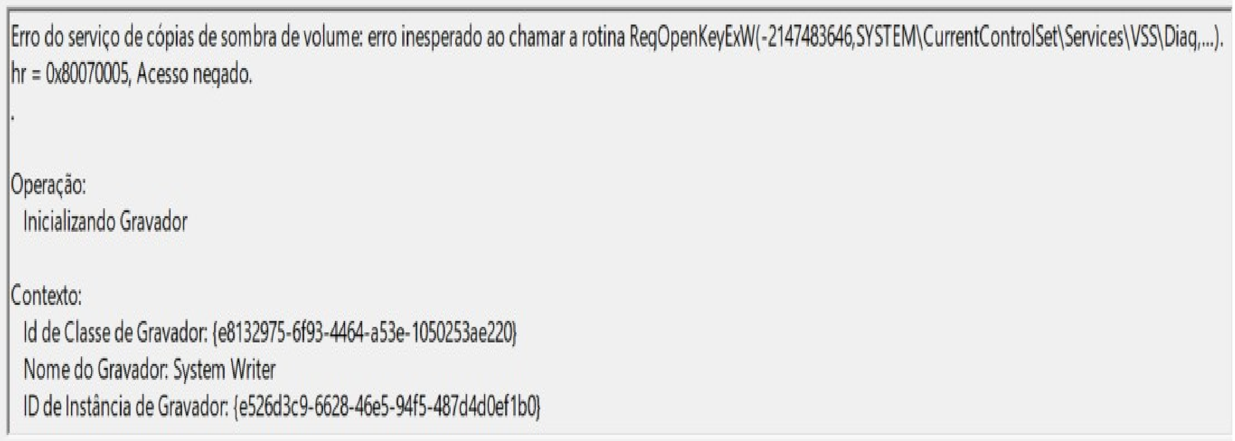
Table 2 – Frequency of Error Events in the 2022/2023 Application Log.

Event Identification	Quantity of occurrences	Category or Description
2004	14623	Could not open the Server service performance object. The first four bytes (DWORD) of the data section contain the status code.
1511	1590	Windows cannot find the local profile and is logging you on with a temporary profile. Any changes you make to this profile will be lost when you log off.
257	632	The volume (partition) was not optimized because an error occurred: (error).
1003	403	LSA/SAM policy change notification was retried and failed. Error 4312 saving the policy change for the account in the default GPOs. For more debugging information, see security\logs\scepol.log in the Windows root.
1023	129	Windows cannot load the extensible counter DLL "WINS" (Win32 error code 4).
1008	112	The Open procedure for service "BITS" in DLL "C:\Windows\System32\bitsperf.dll" failed with error code 8. Performance data for this service will not be available.
8193	109	Volume Shadow Copy Service error: Figure 5.
18221	65	Figure 6.
1000	64	Figure 7.
1026	32	The process was terminated due to an unhandled exception.

Source: Author.

Some notes are as follows, for example, Code 1003 is a Local Security Authority/Security Accounts Manager (LSA/SAM) policy update saving error (Harwood et al., 2023). Codes 1023 and 1008 refer to Dynamic Link Libraries (DLLs), with code 1023 related to Windows Internet Name Service (WINS) (Liang et al., 2025), and code 1008 related to Background Intelligent Transfer Service (BITS), where BITS signals that it failed with code 8, meaning that a DLL is missing or not found (Harwood et al., 2023). Code 8193 is a specific error that occurs when access is denied when initializing a writer (System Writer), giving the context of the identifier, its name, and the instance (**Figure 5**).

Figure 5 – Overview of Event Viewer event 8193.

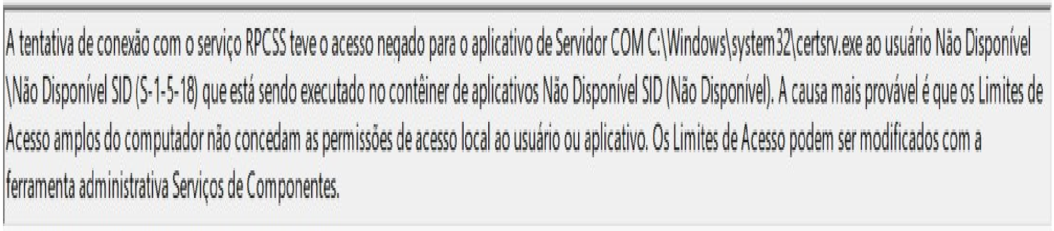


```
Erro do serviço de cópias de sombra de volume: erro inesperado ao chamar a rotina ReqOpenKeyExW(-2147483646,SYSTEM\CurrentControlSet\Services\VSS\Diag,...).
hr = 0x80070005, Acesso negado.
.

Operação:
  Inicializando Gravador

Contexto:
  Id de Classe de Gravador: {e8132975-6f93-4464-a53e-1050253ae220}
  Nome do Gravador: System Writer
  ID de Instância de Gravador: {e526d3c9-6628-46e5-94f5-487d4d0ef1b0}
```

Source: Author.

Figure 6 shows Code 18221, which is an access denied error in Remote Procedure Call(s) (RPC) Service (RPCSS). This code mentions that a COM Server application has been denied access, which means that the user who performed the action or the application does not have permission to perform this procedure.

Figure 6 – General description of event 18221 in the General Tab of the Event Viewer.

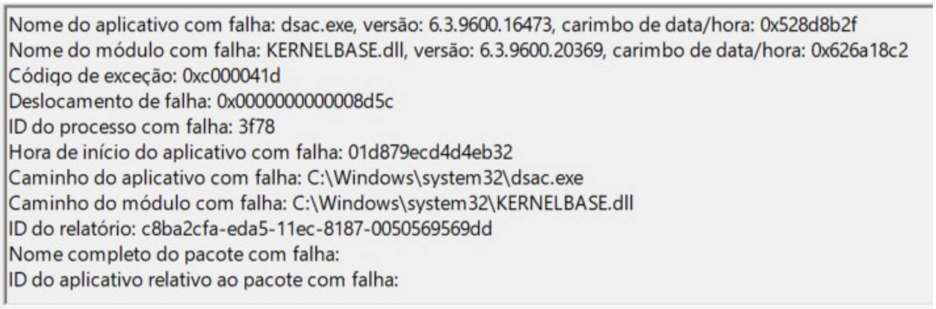


A tentativa de conexão com o serviço RPCSS teve o acesso negado para o aplicativo de Servidor COM C:\Windows\system32\certsrv.exe ao usuário Não Disponível \Não Disponível SID (S-1-5-18) que está sendo executado no contêiner de aplicativos Não Disponível SID (Não Disponível). A causa mais provável é que os Limites de Acesso amplos do computador não concedam as permissões de acesso local ao usuário ou aplicativo. Os Limites de Acesso podem ser modificados com a ferramenta administrativa Serviços de Componentes.

Source: Author.

Figure 7 shows Code 1000, which is an application failure event.

Figure 7 – Event 1000 in the General Tab of the Event Viewer.



```
Nome do aplicativo com falha: dsac.exe, versão: 6.3.9600.16473, carimbo de data/hora: 0x528d8b2f
Nome do módulo com falha: KERNELBASE.dll, versão: 6.3.9600.20369, carimbo de data/hora: 0x626a18c2
Código de exceção: 0xc000041d
Deslocamento de falha: 0x0000000000008d5c
ID do processo com falha: 3f78
Hora de início do aplicativo com falha: 01d879ecd4d4eb32
Caminho do aplicativo com falha: C:\Windows\system32\dsac.exe
Caminho do módulo com falha: C:\Windows\system32\KERNELBASE.dll
ID do relatório: c8ba2cfa-eda5-11ec-8187-0050569569dd
Nome completo do pacote com falha:
ID do aplicativo relativo ao pacote com falha:
```

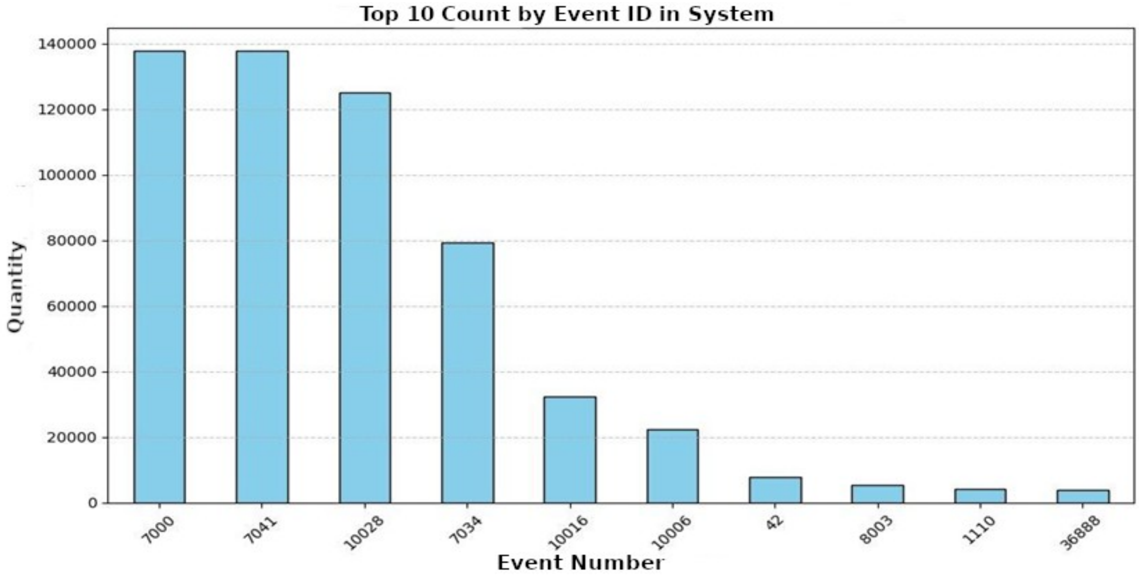
Source: Author.

Other codes within the 1000 range are also called application failure errors, for example, Code 1026 is a .NET Runtime application error, that is, some executable tried to run the .NET framework and had its process terminated due to an unhandled exception.

5.2 Log System Data Collection

In the System Log, the events are distributed in a more linear manner. For example, the first three error codes are 7000, 7041, and 10028, which, according to our analysis, occur at the following frequencies: 24.35%, 24.33%, and 22.10%. Consequently, the respective error codes 7034, 10016, 10006, and 42 occurred at the following frequencies: 13.98%, 5.70%; 3.91%, and 1.34%. Thus, the error codes with less than 1% frequency are: 8003, 1110, and 36888. Figure 8 shows the mentioned codes and the frequency at which they occurred. **Table 3** presents the codes and their descriptions.

Figure 8 – Python Subplot Graph of Event Count in System Logs.



Source: Author.

Table 3 – Frequency of Error Events in the 2022/2023 System Log.

Event Identification	Quantity of occurrences	Category or Description
7000	137813	The Proxy Server (Antivirus) service could not be started due to the following error: The service could not be started due to logon failure, Figure 9.
7041	137732	The service (proxy) could not log on as NT SERVICE\(proxy) with the currently configured password due to the following error: Logon failure: The user has not been granted the requested logon type at this computer.
10028	125117	DCOM could not communicate with the computer (IP) using the configured protocols; requested by PID (PID).
7034	79163	The Network Agent service (Tz0 service) terminated unexpectedly. This has happened (n) times.
10016	32257	The application-specific permission settings do not grant Local Activation permission for the COM Server application with CLSID {CLSID} and APPID {APPID} to the user NT AUTHORITY\IUSR SID (SID) from the LocalHost address (Using LRPC) that is running in the application container Not Available SID (Not Available).

10006	22155	DCOM got an error (error number) from the computer (IP) while trying to activate server: {CLSID}.
42	7639	The description for Event ID 42 cannot be found in the source "Microsoft-Windows-Kerberos-Key-Distribution-Center". The component that generates this event is not installed on the local computer, or the installation is corrupted. You can install or repair the component on the local computer.
8003	5224	The description for Event ID 8003 cannot be found in the source "browser". The component that generates this event is not installed on the local computer, or the installation is corrupt. You can install or repair the component on the local computer.
1110	4035	Group Policy was not processed. Windows could not determine whether the user and computer accounts were in the same forest. Verify that the user's domain name matches the name of a trusted domain in the same forest as the computer account.
36888	3773	A fatal alert was generated and sent to the remote endpoint. This may result in connection termination, Figure 10.

Source: Author.

In this context, codes 7000 and 7041 are similar, as they are both associated with logon failures and related to the functioning of an antivirus. Thus, it can be stated that almost half of the errors recorded in the system (48.68%) are due to failures in the initialization of proxy servers and services. Specifically, code 7000 is linked to problems in the configuration of user privileges, while code 7041 refers to errors in the configuration of the service account. More details about these events are discussed in **Subsection 5.3**.

Additionally, as shown in **Table 3**, code 10016 refers to an error in the ***Component Object Model (COM)***, indicating that a user does not have local permission to run a certain application on his/her machine. Codes 10028 and 10006 are associated with the Distributed Component Object Model (DCOM).

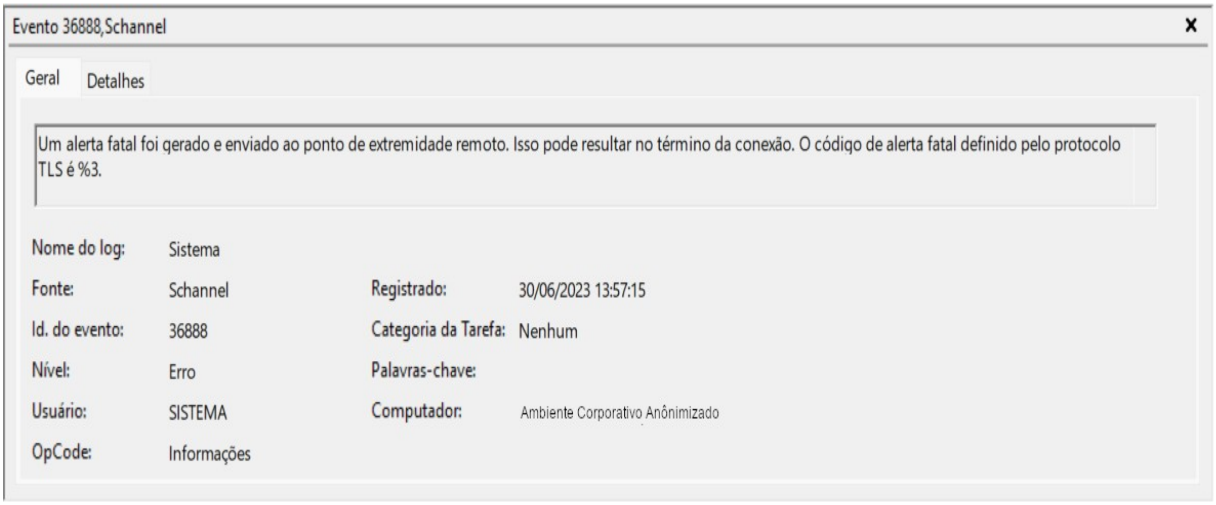
Thus, the Code 10028 indicates a communication failure between DCOM and another machine, while code 10006 represents a recurring error between a client machine and the server, identified and recorded by DCOM itself **(White et al., 2025)**.

Besides that, the Code 7034 counts the number of times a Network Agent service terminated unexpectedly.

Consequently, error codes 42 and 8003 are related to a component not found, namely the Kerberos Ticket Granting Ticket in the case of error 42 and access to the server's server in error 8003. More details on these situations are in Subsection 5.3.

Furthermore, code 1110 is related to a group policy event, that is, Windows does not know whether a user belongs to the domain that AD trusts. Finally, code 36888 consists of a security alert related to the TLS protocol, **Figure 10**.

Figure 10 – Event 36 in the General Tab of the Event Viewer.



Um alerta fatal foi gerado e enviado ao ponto de extremidade remoto. Isso pode resultar no término da conexão. O código de alerta fatal definido pelo protocolo TLS é %3.

Nome do log:	Sistema		
Fonte:	Schannel	Registrado:	30/06/2023 13:57:15
Id. do evento:	36888	Categoria da Tarefa:	Nenhum
Nível:	Erro	Palavras-chave:	
Usuário:	SISTEMA	Computador:	Ambiente Corporativo Anônimizado
OpCode:	Informações		

Source: Author.

5.3 Criticality, Origin and Solutions of Event Errors

The events were evaluated based on a criticality scale from 1 to 5. On this scale, level 1 corresponds to events that do not impact the performance of the user or server services, while level 5 represents incidents that completely interrupt the production of a user or service. Table 4 presents the error events recorded in the application logs, classified according to this criticality scale.

Table 4 – Criticality, Origin and Solution of Error Events in the 2022/2023 Application Log.

Event Identification	Criticality	Source	Solution
1511	5	User Profile Service	Perform backup registry using regedit.exe and delete SID.bak from the login ProfileList.
1003	4	SceSrv	A diagnosis has to be made in “security\logs\scepol.log”.
1000	4	Application Error	Depending on the application, system files, applications, the .NET Framework, or the Operating System must be corrected.
1023	3	Perflib	Fix DLL, software or registry that is causing the problem.
1008	3	Perflib	Re-register the DLL (identified in the event) using regsvr32 and, if necessary, reinstall software related to the DLL.
1026	3	.NET Runtime	Resolve conflicts between the framework and the software causing the problem.
2004	2	PerfNet	Restart the server service.
18221	2	COMRuntime	Update security policies of the server that requires the operation.
257	1	Defrag	There is nothing that needs to be done.
8193	1	VSS	There is nothing that needs to be done.

Source: Author.

In the Application logs, the most critical event identified is code 1511. This error occurs when the user is redirected to a temporary profile, usually due to a corrupted or deleted profile. The fix requires the intervention of an administrator, who must access regedit.exe, make a backup of the registry, and then remove the SID.bak key corresponding to the affected user in the ProfileList section of the Windows Registry. Error events 1003, 1000, 1023, 1008, and 1026 are related to failures in applications, frameworks, or DLL libraries, and may cause specific services to stop. Solutions usually involve reinstalling or updating the affected components. Furthermore, Event 2004 refers to a failure in the system monitoring service. This is a low-critical error, which can be resolved simply by restarting the service. Error 18221 indicates that the user has limited access to server services, and the resolution is by updating the security policies applied to the profile in question. Consequently, Event 257 is generated when the memory slab (system memory allocation area) is insufficient to perform the defragmentation operation. Error 8193, in turn, occurs when network services are removed, resulting in access-denied messages. However, both events are considered low-criticality, as they do not directly impact users or running services. Table 5 shows the error events in the System logs.

Table 5 – Criticality, Origin and Solution of Error Events in the 2022/2023 System Log.

Event Identification	Criticality	Source	Solution
7034	4	Service Control Manager	Reinstall the program responsible for the error.
1110	3	GroupPolicy (Microsoft-Windows-GroupPolicy)	Remediate users and computers in the discovery forest that are experiencing this error event.
36888	3	Schannel	Check the AlertDesc code in the details tab and apply the solution depending on the code (examples: 46, 48, 70).
7000	2	Service Control Manager	Reset privileges of the affected user.
7041	2	Service Control Manager	Check the service account settings and start the service.
42	2	Microsoft-Windows-Kerberos-Key-Distribution-Center	Reset the Kerberos Ticket Granting Ticket account password.
8003	2	bowser	Remove the “browser master” privilege from all users who are not domain controllers.
10028	2	DCOM	Check machine availability for system and review firewall settings.
10006	2	DCOM	Check machine availability for system and review firewall settings.
10016	1	DCOM	There is nothing that needs to be done.

Source: Author.

In the System logs, error 7034 indicates that a program was terminated unexpectedly several times, requiring the affected application to be restarted to restore its functionality. Error 1110 is related to the discovery of forests in the Active Directory. To correct this error, it is necessary to identify the affected user, ensure that the domain controller machines are accessible, and, if necessary, remove and re-add these machines to the domain to re-establish proper communication.

Thus, Event 36888 requires detailed analysis in the "Event Details" tab, where the AlertDesc code indicates the nature of the failure, for example:

1. AlertDesc 40: communication error between client and server;
2. AlertDesc 48: TLS negotiation failure;
3. AlertDesc 70: TLS protocol incompatibility between client and server.

Consequently, correcting these errors involves updating and reconfiguring the TLS protocols on the devices involved. Therefore, error 7000 refers to server services (such as proxy) that fail to start due to a lack of user permissions or privileges. Error 7041 occurs when the service itself does not have logon privileges, and it is necessary to assign this permission to the service user through the Local **Security Policy tool (Secpol.msc)**.

In addition, error 8003 is logged when machines that are not domain controllers assume the role of “browser master” on the network. Although it does not cause a direct impact, this event can generate excessive records in the logs, without any real need for intervention. Errors 10028, 10006, and 10016 are related to DCOM (Distributed Component Object Model), for example:

1. **10028 and 10006** indicate connection failures between the local system and remote machines. To correct this, it is necessary to check network connectivity, machine availability, and firewall settings that may block remote access;
2. **10016** indicates that DCOM components do not have the appropriate access permissions. However, this error usually represents expected behavior and does not require corrective action, being merely informative.

6. Conclusions

This article presents a **case study** based on the analysis of **Active Directory (AD)** logs collected from the live production environment of **Usinas Itamarati (UISA) Company**, which manages approximately 4,000 users in its AD system. The analysis covers a two-year period, from **January 2022 to December 2023**. During the study, the ten most frequent errors recorded in AD were identified and systematically classified into two main categories: **Application Logs** and **System Logs**. Each error was thoroughly mapped, categorized, and visually represented through graphs and tables, considering the following parameters: **a)** Type and class of error; **b)** Frequency of occurrence; **c)** Profile of the users involved; and **d)** Proposed solutions for each incident.

The findings indicate that the structured classification of errors greatly enhanced the ability to detect recurring issues, evaluate their impact on the corporate environment, and devise effective, practical solutions. Thus, the main contributions of this work include:

- Log analysis conducted in a real-world corporate production environment;
- Use of authentic, non-simulated data;
- Evaluation performed over a substantial two-year period;
- Identification and detailed description of the ten most recurrent errors, along with corresponding resolutions;
- Mapping of user profiles involved in critical errors, which represents the core contribution of this study.

For future work, it is recommended that the analysis be extended to include other types of events recorded in AD logs, such as informational events and their sources. This would support the identification of key service, application, and operational demands in corporate environments, providing deeper insights into resource usage patterns and contributing to enhanced infrastructure management and network security.

References

Active Directory: O que é e como funciona? Controle Net, São Paulo, 23 de jun. de 2022. Available at: https://www.controle.net/faq/active-directory/. Accessed on: April 6, 2025.

Active Directory: saiba o que é e como funciona esse recurso. Dinamio, 5 de abr. de 2021. Available at: https://www.dinamio.com.br/blog/2021/04/05/active-directory-saiba-o-que-e-e-como-funciona-esse-recurso/. Accessed on: April 2, 2025.

BARRETO, Jeanine S.; ZANIN, Aline; SARAIVA, Maurício O. **Fundamentos de redes de computadores**. Porto Alegre: SAGAH, 2018. ISBN 9788595027138. Available at: https://integrada.minhabiblioteca.com.br/reader/books/9788595027138/. Accessed on: April 2, 2025.

FOULDS, Iain *et al*. **Visão geral dos serviços de domínio Active Directory**. Microsoft, 8 de mar. de 2023 Available at: https://learn.microsoft.com/pt-br/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview/. Accessed on: April 2, 2025.

FOROUZAN, Behrouz A. **Comunicação de dados e redes de computadores**. 4. ed. Porto Alegre: ArtMed, 2010. E-book. p.i. ISBN 9788563308474. Available at: https://integrada.minhabiblioteca.com.br/reader/books/9788563308474/. Accessed on: April 6, 2025.

GRIPPO, T.; KHOLIDY, H. A. **Detecting Forged Kerberos Tickets in an Active Directory Environment**. ArXiv, 2022. DOI: https://doi.org/10.48550/arXiv.2301.00044.

HARWOOD, Robin et al. **Credentials Processes in Windows Authentication. Microsoft**, 13 de set. de 2023 Available at: https://learn.microsoft.com/en-us/windows-server/security/windows-authentication/credentials-processes-in-windows-authentication. Accessed on: April 6, 2025.

KEYOGEG, Benjamin et al. **Automated detection of ransomware in windows active directory domain services using log analysis and machine learning**. Authorea Preprints, 2024. DOI: 10.22541/au.172779663.36925703/v1.

KUROSE, J. F.; ROSS, K. W. **Redes de computadores e a Internet.** Bookman Editora, 2021. Available at: https://archive.org/details/kurose-redes-de-computadores-e-a-internet-8a/. Accessed on: April 3, 2025.

LAKATOS, Eva M. **Fundamentos de Metodologia Científica**. Grupo GEN, 2021. E-book. Available at: https://integrada.minhabiblioteca.com.br/#/books/9788597026580/. Accessed on: April 2, 2025.

LIANG, Han *et al.* **Erro ou problemas de conexão ao configurar endereços WINS para um servidor WINS**. Microsoft Windows, 15 de jar. de 2025. Available at: https://learn.microsoft.com/pt-br/troubleshoot/windows-server/networking/setting-wins-server-options. Accessed on: April 2, 2025.

MARCONI, Marina de A.; LAKATOS, Eva M. **Metodologia Científica**. Grupo GEN,

2022. Available at: https://integrada.minhabiblioteca.com.br/#/books/9786559770670/. Accessed on: April 2, 2025.

MOKHTAR, Basem Ibrahim et al. **Active directory attacks: steps, types, and signatures**. Electronics, volume 11, número 16, página 2629, 2022. DOI: https://doi.org/10.3390/electronics11162629.

MORAES, Alexandre Fernandes de. **Firewalls: Segurança no Controle de Acesso.** Editora Saraiva, 2015. E-book. ISBN 9788536521978. Available at: https://integrada.minhabiblioteca.com.br/#/books/9788536521978/. Accessed on: April 2, 2025.

MORAES, A. Fernandes de. **Segurança em Redes: Fundamentos**. Ed. Saraiva, 2010. Available at: https://integrada.minhabiblioteca.com.br/#/books/9788536522081/. Accessed on: April 2, 2025.

MOTERO, Carlos Díaz et al. On attacking Kerberos authentication protocol in windows active directory services: A practical survey. **IEEE Access**, v. 9, p. https://doi.org/109289-109319, 2021.

RADAH, Tarek; CHAOUI, Habiba; SAADI, Chaimae. Detecting Unconventional and Malicious Windows Authentication Activities Through Statistical Rarity Assessment. **International Journal of Safety & Security Engineering**, v. 13, n. 5, 2023. DOI: https://doi.org/10.18280/ijsse.130501.

WHITE, Steven *et al*. **Bibliotecas COM, DCOM e Type**. Microsoft, 13 de mar. de 2025. Available at: https://learn.microsoft.com/pt-br/windows/win32/midl/com-dcom-and-type-libraries. Accessed on: April 6, 2025.

WANG, Weifeng et al. **Network attack detection based on domain attack behavior analysis**. In: 2020 13th International Congress on Image and Signal Processing, BioMedical Engineering and Informatics (CISP-BMEI). IEEE, 2020. p. 962-965. DOI: 10.1109/CISP-BMEI51763.2020.9263663.