ALA American Library Association

THE CURRENT LANDSCAPE OF ELECTRONIC RESOURCES ACCESS ISSUES

Ashley Zmau and Holly Talbott

Library Technology Reports
Expert Guides to Library Systems and Services

OCTOBER 2022
Vol. 58 / No. 7
ISSN 0024-2586

Library Technology

R E P O R T S

Expert Guides to Library Systems and Services

The Current Landscape of Electronic Resources Access Issues

Ashley Zmau and Holly Talbott

ALA TechSource

American Library Association

Library Technology
REPORTS

ALA TechSource purchases fund advocacy, awareness, and accreditation programs for library professionals worldwide.

Volume 58, Number 7

The Current Landscape of Electronic Resources Access Issues
ISBN: 9-780-8389-3806-5
DOI: https://doi.org/10.5860/ltr.58n7

American Library Association

225 N. Michigan Ave., Suite 1300
Chicago, IL 60601-7616 USA
alatechsource.org
800-545-2433, ext. 4299
312-944-6780
312-280-5275 (fax)

Editor

Samantha Kundert

Copy Editor

Judith Lauber

Production

ALA Production Services

Cover Design

Alejandra Diaz and ALA Production Services

Library Technology Reports (ISSN 0024-2586) is published eight times a year (January, March, April, June, July, September, October, and December) by American Library Association, 225 N. Michigan Ave., Suite 1300, Chicago, IL 60601-7616. It is managed by ALA TechSource, a unit of the publishing department of ALA. Periodical postage paid at Chicago, Illinois, and at additional mailing offices. POSTMASTER: Send address changes to Library Technology Reports, 225 N. Michigan Ave., Suite 1300, Chicago, IL 60601-7616.

About the Authors

Ashley Zmau has more than ten years of academic library experience and is coauthor of *Electronic Resources Librarianship: A Practical Guide for Librarians* (Rowman & Littlefield 2018) and *The Electronic Resources Troubleshooting Guide* (ALA 2020). She is currently the technical services librarian at Noorda College of Osteopathic Medicine and was previously the electronic resources librarian at the University of Texas at Arlington and the electronic resources management librarian at Southern Methodist University.

Holly Talbott has more than seven years of experience with electronic resources and is coauthor of *The Electronic Resources Troubleshooting Guide* (ALA 2020) and *Electronic Resources Librarianship: A Practical Guide for Librarians* (Rowman & Littlefield 2018). She is currently the electronic resources librarian at Kent State University and was previously the electronic resources and licensing librarian at the University of Arizona Libraries.

Abstract

In this issue of *Library Technology Reports* (vol. 58, no. 7), "The Current Landscape of Electronic Resources Access Issues," we discuss the current landscape of electronic resources access issues through the lens of the prevailing access tool employed by academic libraries: the discovery service. The report outlines the technical components through which library end users gain access to electronic materials through the discovery system environment and describes the common points of failure within them. The report also discusses the troubleshooting techniques and tools through which access issues are identified and diagnosed. The report closes with a discussion on new technological developments in library discovery and access, highlighting the new opportunities for access failure, as well as the initiatives aimed at mitigating these issues.

Contents

Introduction

Electronic resources are a cornerstone of library collections in the modern era. With many libraries offering a robust selection of licensed, purchased, and freely available e-resources, library users have come to expect near-instantaneous access to content from a diverse set of subject areas in a wide range of formats. However, the systems in place to support the discovery and delivery of e-resources to library end users are complex. Depending on a library's system (and how one counts), a user may pass through as many as five or six distinct technology components in order to retrieve the full text of a single journal article. And with these components dependent upon the accurate and timely transfer of data between library, publisher, subscription agent, and discovery vendor, it is unsurprising that libraries and their users experience disruptions in e-resource access.

Troubleshooting e-resource access disruptions has grown as a topic of interest within the library science literature over the past decade. As part of a content analysis of troubleshooting articles published across eight library and information science journals, Lowry noted that the number of published troubleshooting articles has "increased moderately over time," but that ". . . even though the criteria for inclusion in the study included articles published from 2000 to 2020, no articles published earlier than 2010 appeared in the sample" (Lowry 2021, 162). These trends coincided with academic libraries' adoption of discovery services, which arrived on the market in the early 2010s and became largely ubiquitous in the academic sphere by 2018. In his 2018 review on the implementation of discovery systems by academic libraries in the United States, Breeding states that "only 16 percent of the libraries in the group under consideration [had] not yet implemented one of these products (213 out of 1,357)" and that research-intensive universities led the way with only 4 out of 152 institutions (3%) not employing a discovery service (Breeding 2018, 23). As a result of this widespread adoption, most of the discourse surrounding access disruptions and access troubleshooting is predicated on a library utilizing a discovery system as the primary mode of e-resource access for its end users.

For this technical report, we discuss the current landscape of electronic resources access disruptions through the lens of the prevailing access tool employed by academic libraries: the discovery service. The report outlines the technical components through which library end users gain access to electronic materials through the discovery system environment and describes the common points of failure within them. The report also discusses the troubleshooting techniques and tools through which access issues are identified and diagnosed. The report closes with a discussion on new technological developments in library discovery and access, highlighting the new opportunities for access failure, as well as the initiatives aimed at mitigating these issues.

References

Breeding, Marshall. 2018. "Index-Based Discovery Services: Current Market Positions and Trends." *Library Technology Reports* 54, no. 8 (November/December): 1–33. https://doi.org/10.5860/ltr.54n8.

Lowry, Lindsey. 2021. "Exploring the Evidence-Base for Electronic Access Troubleshooting: Where Research Meets Practice." *Journal of Electronic Resources Librarianship* 33, no. 3: 156–69. https://doi.org/10.1080/1941126X.2021.1949153.

Components of E-resource Access

The technologies employed to deliver library e-resource access to end users have evolved considerably over the past decade. Within the academic library sphere, online public access catalogs (OPACs) and federated search interfaces have given way to "web-scale" index-based discovery systems; e-resource holdings and linking information are now administered within cloud-hosted knowledge management systems rather than locally hosted integrated library systems (ILSs); and user authentication has expanded to include a variety of IP and federated identity management (FIM) options. In order to facilitate the discussion around e-resource access disruptions, we begin with a chapter on these technological developments. In this chapter, we define the technology components through which library end users gain access to electronic materials, focusing on those that comprise the discovery service environment. We describe how each component works, the role it plays within the larger library system, and how metadata from these key systems plays an integral role in e-resource access. We also discuss the different types of metadata, the systems from which they originate, and the spheres of control that govern their management.

Search and Discovery

Library systems consist of four basic components: search and discovery (access) tools, knowledge management systems, linking systems, and authentication. Regardless of how a library configures its system, these four pieces must be present to enable e-resource access. We begin by discussing search and discovery.

Terminology

- *Access tools,* sometimes called discovery or retrieval tools, are any computer application through which a library user can discover and gain access to an e-resource. Features and functionality vary greatly from tool to tool, and libraries typically employ multiple tools to meet a variety of access needs. Types of access tools include online public access catalogs, database A–Z lists, e-journal A–Z lists, and web-scale discovery services.
- *Central or discovery indexes* are collections of "pre-harvested and processed metadata and full text that comprises the searchable content of a [web-scale discovery] service" (Hoeppner 2012, 7). These indexes harvest and normalize vendor-supplied resource data, which can include "rich" metadata such as abstracts, author-supplied keywords, tables of contents, and full text. It is these indexes that power web-scale discovery services.
- *Database A–Z lists* are alphabetical lists of databases (and other selected e-resources) to which a library provides access. Libraries create these lists through a variety of methods, which range from manually adding hyperlinks to a static web page to developing a homegrown database solution to employing a vendor product, such as Springshare's LibGuides A–Z Database List.
- *Discovery interfaces* are search applications that ingest and index metadata from a variety of sources, including institutional repositories, digital collections, and APIs (Breeding 2018). They provide users with advanced search features, such as keyword recommenders, limiters, facets, and relevancy ranking of results. These features are meant to encourage more serendipitous discovery rather than strict known-item retrieval.
- *Discovery services,* sometimes called index-based discovery services or web-scale discovery services, are products that combine a discovery interface with a central index. Unlike a standalone discovery interface, a discovery service facilitates the discovery of resources outside of a library's holdings via its connection to a central

or discovery index or indexes. It also allows for article-level and chapter-level search results and linking.

- *E-journal A–Z lists* are alphabetical lists of electronic journals to which a library provides access. These lists are typically auto-populated according to the library's holdings. Besides acting as a searchable inventory of a library's e-journals, an A–Z list also collates and displays each e-journal's available access points, as well as other relevant information, such as coverage dates and notes regarding licensing and authentication.

Discussion

Index-based discovery services have become the most widely adopted discovery application by academic libraries. Previously, most libraries employed online public access catalogs through which library users could search locally maintained metadata records. OPACs were quickly found to be insufficient to support e-resource access because these resources morphed and multiplied more rapidly than individual libraries could maintain them. This created constant errors and inaccuracies within OPACs and led to frustration by librarians and library users alike. Discovery services, by contrast, reduce the pressure on individual libraries to keep up with the constant flux of e-resource metadata. By utilizing repositories of e-resource metadata compiled and maintained by a discovery service vendor, libraries are able to provide more robust and up-to-date coverage of their e-resource holdings, as well as delivering a more granular (and Google-like) search experience to users.

The discovery service market is dominated by a handful of commercial vendors that host and maintain the discovery service on behalf of their library customers. Discovery service search results are populated from centralized indexes, which have ingested and normalized data from hundreds of publishers, aggregators, and content providers. Content included in these indexes comes from both open-access and commercial sources and encompasses everything from e-books and e-journals to video, images, sound recordings, government documents, and more. Discovery services also facilitate the discovery of local catalog and institutional repository records, which can be contributed by the library via FTP or OAI-PMH protocol.

Because central indexes harvest metadata from hundreds of content providers, many of which have their own standards for representing e-resource information, the accuracy and quality of the ingested metadata vary from provider to provider. Similarly, what and how much data is shared by content providers is governed by their contracts with the discovery service vendor. Some content providers, for instance, authorize their data to be utilized only by subscribing institutions. Discovery service vendors that also act as content providers (e.g., EBSCO and ProQuest/Ex Libris) are unwilling to exchange metadata in order to preserve a competitive edge for their discovery product. This has led to opaqueness around both the discoverability of e-resources within a library's chosen discovery service and how the robustness (or meagerness) of the data within the central indexes has influenced e-resource usage.

Academic libraries have supplemented their use of discovery systems with additional access tools for more targeted discovery needs. OPACs, for instance, are sometimes employed in tandem with a discovery service and are used primarily for known-item searching. Other common access tools used by libraries include database A–Z lists, which are popular for giving end users an easy-to-scan list of their library's available online databases. E-journal A–Z lists fulfill a similar function for the discovery of electronic journals, allowing for the easy search and retrieval of known serials titles. These access tools are maintained either independently by the library (as with Springshare's LibGuides A–Z Database List) or as part of a broader knowledge management system, which we discuss next.

Knowledge Management Systems and Link Administration

Terminology

- *Direct linking* refers to the creation of links within a discovery service by leveraging provider-specific, proprietary metadata from the central index. Direct linking is usually employed by discovery services alongside link resolver/OpenURL linking because it "provide[s] more reliable access to electronic resources than through the OpenURL process" (Breeding 2018, 7).
- An *ERMS*, or electronic resource management system, is a knowledge management system that specializes in tracking and managing electronic resources throughout their life cycle. An ERMS is typically powered by a centralized knowledge base, which allows librarians to easily find and activate specific instances of e-resources or e-packages, and includes additional management features, such as the ability to store payment, licensing, and contact information; to receive renewal reminders; and to track usage.
- An *integrated library system* is a suite of modules used by librarians to manage the activities involved in acquiring and loaning materials, such as ordering, invoicing, cataloging, and circulation. ILSs were originally developed to provide

operational support for physical materials and as a result are poorly equipped to handle the complexities of e-resource management. These inadequacies have prompted the development of other tools, such as ERMSs, A–Z lists, and library services platforms (LSPs).

- *Knowledge bases* are centralized databases of metadata that describe specific instances of e-resources available through a publisher, content provider, or platform (Wilson 2016). A knowledge base includes not just basic bibliographic information (title, author, publisher, etc.) but also information about the resource's platform, vendor, coverage dates, and access model, including which packages or collections it appears in. Knowledge bases are used to power a variety of knowledge management systems and access tools. The primary purpose of the knowledge base is holdings management, allowing libraries to track which e-resources they have with certain vendors. This, in turn, supports the article-level links users encounter in a library's discovery service and the title-level links in a library's A–Z lists.
- *Link resolver,* or OpenURL linking, refers to the "specialized software used to provide context-sensitive links among the panoply of systems that compose a modern library's electronic collections" (Chisare et al. 2017, 93). Utilizing the OpenURL encoding format, link resolvers create their links by combining the citation data of the desired resource (source) from a library discovery record with the provider website (target) linking parameters necessary to connect to the desired resource. For a link resolver to know which resources are locally available to a library user, it must be connected to a knowledge base that has been pre-populated with a library's electronic holdings.
- *LSP* refers to a next-generation library system that incorporates the functionalities of an ILS, a knowledge base, a link resolver, and an ERMS. Library services platforms were developed as a way to unite the disparate knowledge management systems into one comprehensive system and support the workflows of electronic, digital, and physical material.

Discussion

As e-resources increased in availability, it quickly became clear that integrated library systems were inadequate to support the maintenance of electronic holdings. While e-resource MARC records could be loaded into ILSs, the accuracy of these records decreased as the overall number of records increased. Vendor participation in holdings workflows was often limited to supplying a library with MARC records, and these records frequently needed remediation to bring them up to cataloging standards. Thus, the onus of holdings maintenance rested entirely on local libraries. The sheer volume of data that needed to be maintained quickly became overwhelming for libraries without the staff or time available to offset the cumbersome workflows.

The proliferation of electronic resource management systems in the mid-2000s further enticed libraries away from traditional models of holdings management. ERMSs are stand-alone systems connected to a link resolver knowledge base, which provided context-sensitive links to e-resource content. The advent of link resolvers and their attached knowledge bases became a panacea for the historical efforts of loading individual MARC records for e-resources. Companies such as Serials Solutions provided knowledge bases that could be used to track the collections, packages, and individual subscriptions available to a library. These knowledge bases also could be connected to a discovery service to provide a single-search experience for users to find both e-resource and print content, as well as retrieve more granular results, such as at the article or chapter level.

While a mix-and-match approach to discovery is available, libraries tend to procure their ERMS, link resolver, and discovery service as a suite of products from the same vendor. This trend of bundling services is likely to continue into the foreseeable future as the discovery industry continues to consolidate, leaving libraries with fewer vendors to choose between. Next-generation library systems take this one step further with the library services platform, which combines the functionality of an ERMS/knowledge base with that of a traditional ILS, providing a unified place to administer both print and electronic resources. While LSPs are still in their infancy, they promise to reduce the number of disparate systems needed by electronic resources librarians to effectively manage their e-resources.

Authentication

Terminology

- *Authentication* is the process of proving one's identity as an authorized or legitimate user of a product or service. Most vendors and content providers require that users first prove their affiliation with the purchasing or subscribing library before they are allowed to access content on the platform. Libraries employ various methods of authentication, including via IP address, proxy server, virtual private network (VPN), and single sign-on (SSO).

- *Proxies* are a type of intermediary server or software system that sits between one computer and another. Libraries commonly employ proxies to authenticate remotely located users because a proxy enables a library to override a computer's IP address with its own, thus changing the computer's apparent location. The most commonly employed proxy system for libraries is EZproxy.
- *Federated identity management*, or federated SSO, refers to a system of single sign-on that enables users to authenticate into applications across multiple unrelated third-party domains using a single set of credentials. With federated identity management, a user's credentials are verified by a trusted identity provider (often the user's educational institution), which then communicates the user's authentication status to third parties via a secure protocol, such as SAML or OAuth. FIM enables library users to authenticate into multiple content provider platforms using a single set of credentials without the need for IP addresses, proxies, or VPNs. Common identity federations include InCommon (for Shibboleth SSO) and OpenAthens.
- *Multifactor authentication*, or two-step authentication, is an authentication method in which a user verifies their identity using additional pieces of information beyond their username and password. This information may be the answer to a security question, a security code sent to a verified e-mail address or phone number, or acknowledgment of the log-in attempt via a third-party application.
- *Single sign-on* is a form of authentication that uses session information stored as a cookie on a web browser to automatically authenticate a user into multiple applications within the same organization after the user has logged in once. Single sign-on is frequently used by higher education institutions to reduce the number of times a user needs to authenticate into applications hosted or provided by the institution. It is increasingly used in conjunction with multifactor authentication to provide added account security.
- *VPNs,* or virtual private networks, are services that create a secure, encrypted connection from one computer to another. Similar to a proxy, a VPN acts as a middleman for a computer and its destination, sitting between them and overriding the connecting computer's IP address with its own. However, unlike a proxy, a VPN is more secure because it encrypts a computer's information before it even connects to the internet.

Discussion

IP authentication is currently the most popular way to authenticate library users. When a library acquires an e-resource, it provides the vendor with a set of IP ranges that represent the library's computer and Wi-Fi network. When a user connects to the e-resource over the internet, the vendor checks the device's IP address to see if it falls within the provided ranges. If it does, the user is granted access. If not, the user is redirected to an error or a payment message. Since this process happens behind the scenes, the user is never prompted to enter credentials, making the movement from discovery record to e-resource appear seamless. Unfortunately, IP authentication by itself is able to provide access only for users who are currently located on the library's or institution's physical site. As a result, IP authentication is frequently used in conjunction with other authentication methods to grant access to users who are located remotely.

Many libraries employ a proxy service jointly with IP authentication to enable e-resource access to users located outside the library's physical premises. When a remotely located user attempts to connect to an e-resource through one of the library's access tools, the browser is redirected to the proxy server, which asks for the user's credentials. The browser redirect can happen a couple of different ways but typically involves modifying the e-resource's URL, such as adding a prefix to the beginning of the e-resource's URL. Once the proxy verifies the user's credentials against its internal database, it connects the browser to the desired resource using its own IP address. Since the proxy server's IP address is included in the authorized ranges given to vendors, the user is granted access to the e-resource. In addition to the proxy prefix, a proxy requires maintenance of several configuration files to function, including one that contains the URLs, hosts, and domains of the e-resource's platform. The configuration file needs to be frequently updated to keep pace with vendor platform developments.

Another way to provide access to remote users is through a VPN, or virtual private network. A VPN fills a similar role as a proxy, acting as an intermediary between the user's device and the desired e-resource. Just as with a proxy, a user's device must first connect with the VPN, thus assuming its IP, before connecting to the e-resource. Because the VPN's IP address is included in the ranges provided to the vendor, the device appears to be located on site and is authorized for access. However, unlike a proxy, a VPN requires users to download and install specialized software onto their personal devices, configuring it with settings specific to their institution. But not all institutions' VPN services are configured to provide access to e-resources. Some institutions implement a practice called split tunneling, which means the VPN routes only certain types of web traffic through its server, while the rest access the internet normally. Institutions that use split tunneling generally route only traffic destined for internal resources, such as those

Table 2.1. Sources and types of metadata

Component	Sources of Metadata	Types of Metadata	Sphere of Control
Online Catalog/ILS	• Original MARC record cataloging • Individual MARC record loads • Bulk MARC record loads	• Bibliographic metadata • Database/collection citation metadata • Book citation metadata • Journal citation metadata • Video citation metadata • URLs	Library
Central Index	• Data supplied by publishers, vendors, and content providers	• Bibliographic metadata • Video citation metadata • Article citation metadata • Abstracts • Full text • Direct links • DOIs • Table of contents	Vendor
Knowledge Base	• Data supplied by publishers, vendors, and content providers	• Bibliographic metadata • Database/collection citation metadata • Book citation metadata • Journal citation metadata • Video citation metadata • Parser & parser parameters • Link resolver information	Vendor
Discovery Service	• Online catalog/ILS • Central index • Knowledge base • APIs	• Bibliographic metadata • Database/collection citation metadata • Book citation metadata • Journal citation metadata • Video citation metadata • Article citation metadata • Abstracts • Full text • Direct links • DOIs	Blended
Library Services Platform	• Original MARC record cataloging • Individual MARC record loads • Bulk MARC record loads • Knowledge base	• Bibliographic metadata • Database/collection citation metadata • Book citation metadata • Journal citation metadata • Video citation metadata • Parser & parser parameters • Link resolver information • Site IDs	Blended
Link resolver	• Knowledge base	• Citation information • Parser & parser parameters • Link resolver information	Vendor
ERMS	• Selection of holdings from a knowledge base	• Bibliographic metadata • Database/collection citation metadata • Book citation metadata • Journal citation metadata • Video citation metadata • Site IDs	Blended
Database A-Z List	• Manual record creation	• Database/collection title • URLs	Library
E-journal A-Z List	• Auto-populated from holdings selected from a knowledge base	• Journal citation metadata • Holdings/coverage dates • URLs	Blended
Research Guide	• Manual entry • Asset management tool	• Database/collection title • Book title • Journal title • Video title • URLs	Library

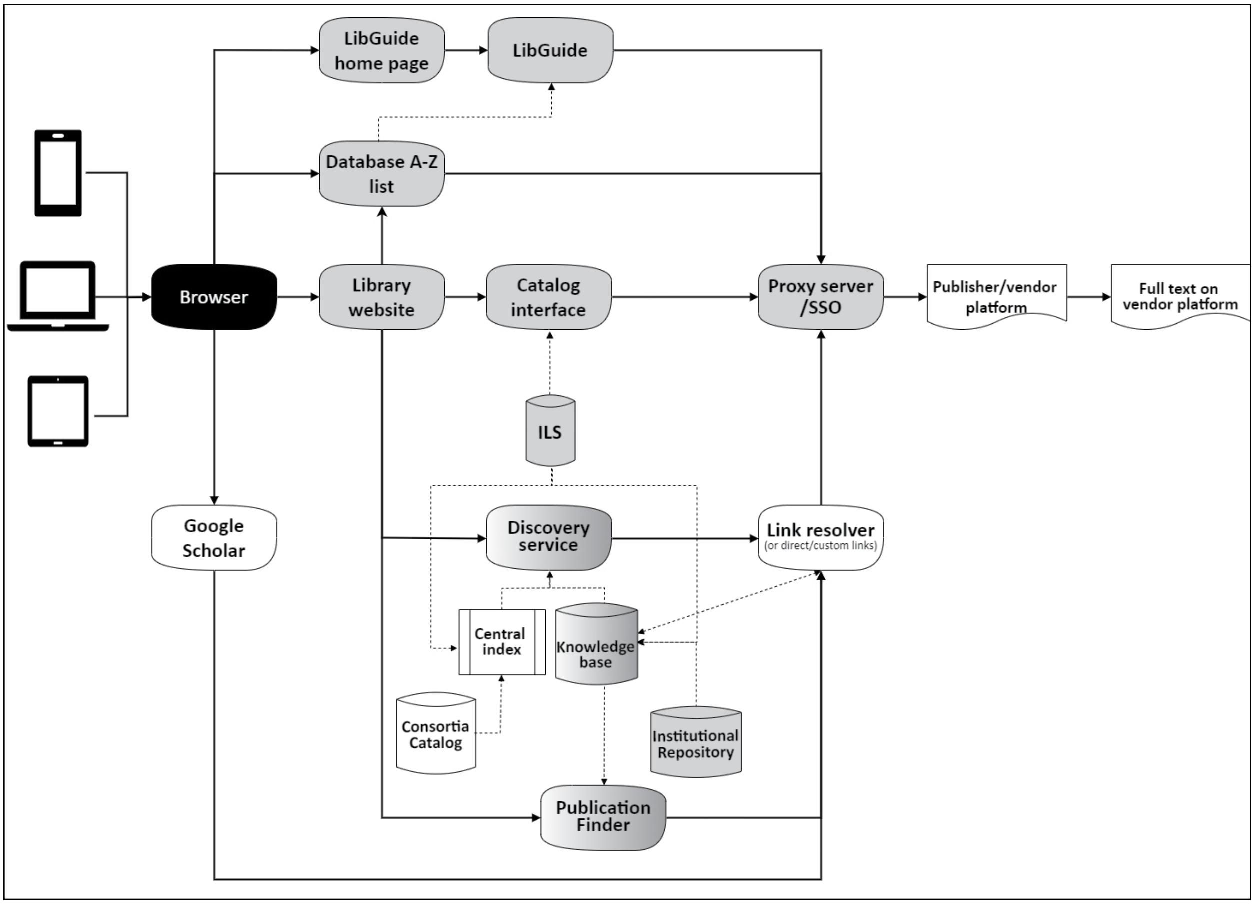

Figure 2.1
Comprehensive access chain. Black = patron-controlled metadata, system, or tool; gray = library-controlled metadata, system, or tool; white = vendor-controlled metadata, system, or tool; gradient indicates shared control.

hosted on the institutions' intranet, through the VPN; all other traffic, including that going to library e-resources, accesses the internet using the user's normal router and IP address. This means if the user is off site, they will not be authenticated correctly.

While IP authentication remains widely employed by academic libraries, federated identity management (FIM) authentication continues to grow as a preferred method of authentication by academic libraries and vendors due largely to its ability to provide more account security, such as through multifactor authentication. With FIM authentication, a user can navigate to an e-resource from anywhere on the internet, including Google, and be able to log in by choosing their institution from the provided drop-down menu, often called a WAYF (Where Are You From), on the vendor's platform. Once a user logs in, the information (called a token) is stored as a cookie on the browser, which can then be shared by other resources and vendors without the user needing to log in again. Because FIM requires vendors to join an identity federation, such as InCommon (Shibboleth) or OpenAthens, as well as install and configure additional software on their servers, not every vendor will have it as an option. As a result, FIM is often used in conjunction with other authentication methods such as proxy to provide robust coverage.

Sources and Types of Metadata

A significant portion of e-resource access disruptions is derived from incorrect metadata. Bibliographic, holdings, and platform information form the backbone of all library access and linking tools. This means any missing, erroneous, or out-of-date metadata will adversely affect the discoverability of an e-resource and potentially lead to breakdowns in access. However, metadata can originate from a number of sources, including internally within the library or externally with a publisher, content provider, or discovery vendor. It is also often blended together within individual access tools, making it difficult to pinpoint where the metadata came from, what portion is causing an access issue, and which party is responsible for correcting it. Understanding the flow of metadata from its various origination points is therefore essential.

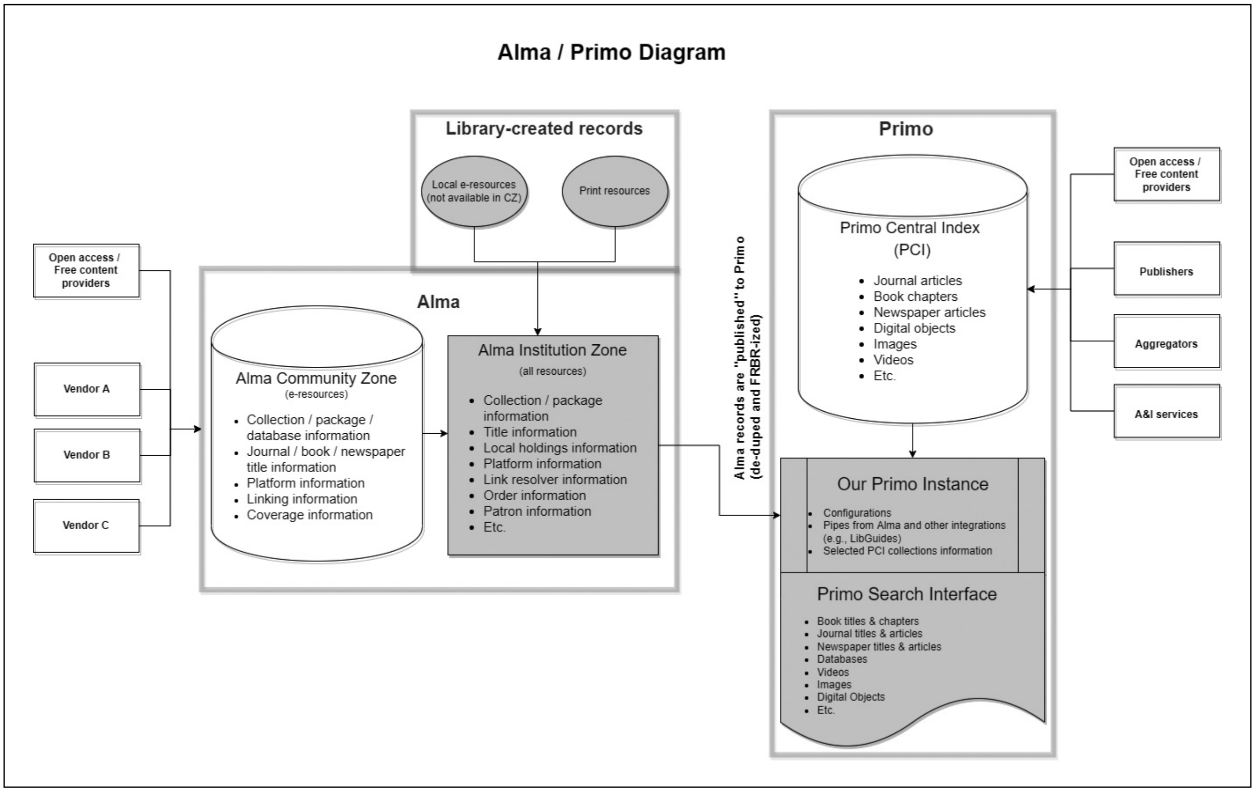

Figure 2.2
Library services platform: Alma/Primo access chain. White = Ex Libris or vendor-controlled metadata; gray = library or blended controlled metadata.

Table 2.1 (p. 10) summarizes the sources and types of metadata that feed into each component in the comprehensive access chain. We have also included a rough guide to whose sphere of control each falls under: library, vendor, or a blend of the two. This distinction is important because depending on whose sphere of control the component falls under, a troubleshooter will have a greater or lesser ability to test hypotheses, effect change, and enact solutions. This table is solely focused on e-resource metadata and therefore does not take into account other sources of print, digital, or institutional repository metadata. Also, please note that the table is not exhaustive and represents only metadata found to be the most commonly used for diagnosing e-resource access disruptions.

Comprehensive Access Chain

Figure 2.1 (p. 11) depicts how search and discovery (access) tools, knowledge management systems, linking options, and authentication methods work together to enable access to a library's electronic resources. The diagram details a few paths a user may take through the chain of access (solid line), as well as the flow of metadata between the various components (dotted line). It includes an example of how users can begin their discovery journey outside of the library website with Google Scholar, which can be configured to utilize the library's link resolver to connect users to the library's holdings. Other abstract and indexing (A&I) databases offer similar functionality, but it is up to individual subscribing libraries to decide which platforms it is enabled on. Figure 2.2 depicts how the same technology components are utilized in a library services platform, in this case Ex Libris's Alma/Primo.

References

Breeding, Marshall. 2018. "Index-Based Discovery Services: Current Market Positions and Trends." *Library Technology Reports* 54, no. 8 (November/December): 1–33. https://doi.org/10.5860/ltr.54n8.

Chisare, Cyndy, Jody Condit Fagan, David Gaines, and Michael Trocchia. 2017. "Selecting Link Resolver and Knowledge Base Software: Implications of Interoperability." *Journal of Electronic Resources Librarianship* 29, no. 2: 93–106. https://doi.org/10.1080/1941126X.2017.1304765.

Hoeppner, Athena. 2012. “The Ins and Outs of Evaluating Web-Scale Discovery Services.” *Computers in Libraries* 32, no. 3 (June 24): 6–40. https://www.infotoday.com/cilmag/apr12/Hoeppner-Web-Scale-Discovery-Services.shtml.

Wilson, Kristen. 2016. “The Knowledge Base at the Center of the Universe.” *Library Technology Reports* 52, no. 6 (August/September): 1–35. https://doi.org/10.5860/ltr.52n6.

Overview of Common Issues and Symptoms

Library science has tackled identifying trends in e-resource access disruptions from a number of vantage points. Many articles have focused on assessing errors resulting from specific technology components, including OpenURL linking, knowledge base metadata, authentication systems, gaps in web-scale discovery coverage, or the usability of discovery services. Others have approached access disruptions through the broader lens of e-resource troubleshooting. Less has been written on attempts to understand access disruption trends holistically, such as through help ticket analyses. Lowry, for instance, notes that only five of the thirty-five articles included in her content analysis of troubleshooting articles "utilized a method of analysis wherein troubleshooting tickets or reports were analyzed in some way" (Lowry 2021a, 165). Similarly, a recent survey of academic libraries showed that while 51 percent of the 143 respondents were tracking e-resource access issues reported at their institutions, only 15 percent had conducted a formal analysis of that data (Lowry 2021b). While strides have been made in recent years to standardize the language around access disruptions, the field is just beginning to develop a shared framework around which the rates and categories of access problems can be compared across institutions.

Without such comparative analyses, it can be difficult to state with certainty which e-resource access disruptions are the most prevalent. Here, discovery and content vendors could help fill in the gaps, contributing to the field with their own analyses of access issues reported and resolved via their support centers. These analyses do not seem to be forthcoming. Instead, librarians must rely upon personal experience, anecdotal stories, and individual case studies to spot larger trends in access disruptions. Fortunately, as Brett states, "Any practitioner who regularly addresses e-resource access problems knows there are common 'types' of problems" (Brett 2018, 198)—and that is what we will discuss in this chapter.

Literature Summary

The earliest studies to attempt to holistically assess the frequency and types of e-resource access disruptions throughout a library's system were availability studies. Availability studies utilize a method of systematic analysis to evaluate how well a library fulfills user item requests. Initially developed to evaluate the availability of physical items in library collections, these studies were subsequently adapted to incorporate e-resource access by Nisonger (2009), Crum (2011), and Mann (2015). In each study, the researchers searched for the full text of a predetermined sample of e-resource citations using either the library catalog or A&I databases equipped with the library's OpenURL link resolver. The results were then analyzed to determine the rate of success finding the full text and to identify trends that contributed to the failures. Mann (2015) is particularly noteworthy for being one of the first to develop a conceptual model to categorize e-resource access failures, as well as the first to attempt to quantify the effectiveness of troubleshooting by comparing availability results before and after error remediation. Mann and Sutton (2015) followed up this study with another incorporating aspects of usability testing, resulting in an expansion of Mann's original concept model to include both system and human errors.

During the same year, studies analyzing access disruptions reported via help tickets, chat transcripts, and ILL requests began to emerge. Browning (2015) analyzed problem-report e-mails received from March through December 2013 by Auroria Library; Wright (2015) reported on findings from a study of University of Michigan's new problem ticket tracking system at ALA midwinter; Ashmore, Allee, and Wood (2015) used canceled ILL requests during the 2012–2013 school year at Samford University Library to identify link resolver errors; Ashmore and Macaulay (2016) expounded upon the results of the 2015 study to identify three core types of link resolver problems; Goldfinger and Hemhauser (2016) studied a random sampling of problem tickets submitted between March 2010 and October 2013 at the University of Maryland, College Park; Enoch (2018) analyzed error reports submitted for e-resource access issues within the University of North Texas Libraries' discovery service; Kimbrough (2018) analyzed chat transcripts to identify e-resource problems frequently encountered by patrons at Georgetown University Library; Baskaran (2019) examined chat transcripts at North Carolina State University Libraries to identify e-resource access problems for further investigation; Lounsberry, Wood, and Thornton (2021) used ILL data at LSU to identify access issues in a proactive manner; and, finally, Foster (2021) categorized problem alert tickets in JIRA using a locally developed controlled vocabulary at Ohio State University. The metrics and disruption trends gathered during these studies were used to inform many local practices, including decisions on cleanup projects, staff time allocations, troubleshooting workflows, and acquisitions.

Like Foster (2021), many of these studies developed local schemata to classify their access issues within their analyses. However, as Browning (2015) points out, the classification process was often time-consuming and "allowed for personalization and creativity" (32), resulting in subjective, institution-specific categories. Goldfinger and Hemhauser expressed the limitations of these localized schemata, stating the "lack of controlled vocabulary for problem types among librarians impedes the ability to compare e-resource access problem experiences with other institutions," specifically describing their efforts to compare the University of Maryland's results to similar analyses at other institutions as "comparisons of 'apples to pears' rather than apples to apples" (Goldfinger and Hemhauser 2016, 92). In response, they offered up their own classification schema as a standardized way to describe and categorize e-resource access issues.

Brett (2018) subsequently used their categorizations to classify 305 help tickets at the University of Houston Libraries and compare the results to that of the University of Maryland, College Park. Brett concluded that the results "demonstrate that libraries experience similar types of access problems across institutions" and that "a standardized vocabulary for categorizing e-resource access problems would benefit the profession by improving troubleshooting practices and problem reporting to vendors" (Brett 2018, 203). Similarly, Lowry (2020) utilized Goldfinger and Hemhauser's classification schema to code troubleshooting tickets at the University of Alabama Libraries in order to compare findings among the three research institutions (University of Houston, University of Maryland, College Park, and the University of Alabama). The study confirmed that "certain types of access problems do occur at similar rates among research institutions, despite the likely differences in workflows, tools, management styles, and varying collections among them" and that the "two most common problems at all three libraries fell into the categories of KB/Link Resolver or Platform" (Lowry 2020, 29, 31). Finally, Gould and Brett (2020) performed a similar analysis for help tickets at Texas A&M University (TAMU) and the University of Tennessee, Knoxville (UTK) and discussed the results in comparison to previous studies. They discovered that "KB/Link Resolver, platform-related, and user-error access problems each accounted for large percentages of total problems at both institutions" (Gould and Brett 2020, 195), a result consistent with the findings of Goldfinger and Hemhauser (2016) and Brett (2018). Proxy- and IP-related problems were also flagged as constituting a large percentage of the reported issues.

Common E-resource Access Issues

Device and Network

The search and discovery process always begins with a user's individual technology components—that is, user- or patron-controlled components. This includes items like the user's device, internet or network connection, browser, and browser settings. E-resource access issues originating within these components can present symptoms anywhere throughout a user's discovery journey but are typically experienced at either the very beginning or the very end of the process. The symptoms also frequently cannot be reproduced by the troubleshooter, which can make diagnosing them quite difficult. Since access issues originating from user-controlled components are particular to the user's device and network setup, they require action by the user in order to be resolved. Thus, they are considered to be within the user's sphere of control.

Common causes and symptoms originating from each component include the following:

- Device
  - Causes
    - The user's device is running an old or unsupported operating system.
    - The user's device does not have the appropriate software for viewing or interacting with the library resource (e.g., does not have

a PDF viewer or reader with DRM software, such as Adobe Digital Editions, installed).
    - Symptoms
        - Slow upload and download times.
        - Inability to open or view downloaded file types.
- Network and internet connectivity
    - Causes
        - The user's network connection is slow, spotty, or experiences high latency (delays in transmitting and processing network data; this is common with satellite internet).
        - The user's satellite internet service providers' proxy or VPN (used to mitigate latency issues) interacts negatively with the library's authentication system, such as EZproxy.
        - The user's network utilizes firewalls or other network security features that interact negatively with the library's authentication system.
    - Symptoms
        - Timeout errors.
        - Lag.
        - Slow upload and download times.
        - Dropped proxy or authentication.
- Browser and browser settings
    - Causes
        - The user is using an older browser or a browser unsupported by the vendor platform.
        - The data stored in the browser's cache or cookies is interacting negatively with the vendor platform or library resource.
        - The browser's pop-up blocker is preventing content from loading, or the browser's security settings are blocking safe sites from being accessed.
    - Symptoms
        - Slow loading times.
        - Content or web pages not loading on the vendor platform.
        - Error messages or security warnings.

Discovery Service

A library's discovery service is usually powered by three main reservoirs of metadata: the ILS or catalog, knowledge base, and central indexes.

CATALOG

Access disruptions originating from a library's catalog or ILS generally concern locally controlled MARC records containing incorrect or incomplete bibliographic information, coverage dates, or URLs. MARC records may have also been erroneously loaded or unsuppressed for content the library does not currently own or subscribe to. When library users encounter faulty metadata from these MARC records within their OPAC or discovery service, they may experience

- broken links
- proxy error messages
- missing or unnecessary prompts for authentication
- paywalls on the vendor platform

Fortunately, once the problem is isolated to the appropriate MARC record, a troubleshooter is able to take swift action to resolve the issue because these records are typically managed by the library itself. This is often not true when it comes to knowledge bases and central indexes.

KNOWLEDGE BASE

Unlike a catalog, a knowledge base contains more than just bibliographic metadata; it also contains data that describes specific instances of e-resources, including the resource's platform, vendor, coverage dates, and access model, such as which packages or collections it appears in. Since the knowledge base receives this data directly from publishers or content providers, each of which has its own internal standards for representing e-resource information, the quality of the metadata can vary from provider to provider. Some knowledge base vendors attempt to augment or normalize this data in order to keep it consistent across providers, but this process can also introduce additional errors. Furthermore, providers frequently make changes to their platforms, the content of those platforms, and the way that content is packaged and sold to libraries, making it difficult for knowledge base vendors to keep up with the changes. As a result, there is often a lag time between when a collection or resource is modified on the provider's platform and when its metadata is modified within the knowledge base. This can result in scenarios such as the following:

- broken links caused by outdated URLs or incorrect linking information
- broken links caused by incorrect bibliographic or citation information (e.g., wrong ISSN/ISBN)
- links defaulting to a provider's home page instead of the individual article or title
- packages missing titles that have been added
- packages including inaccessible titles or titles that have been removed

Because a knowledge base is often utilized in a number of components, including ERMSs, discovery services, link resolvers, and e-journal A–Z lists, these symptoms can display in several places. This means testing access via different access tools may result in the same error message or broken link. Not only does this limit the alternative routes troubleshooters can provide to problem reporters for accessing their desired content, but it also prevents troubleshooters from cross-checking the metadata within the library's access infrastructure. Instead, troubleshooters will need to do that through an outside source, such as OCLC or Ulrich's Periodicals Directory, or by going directly to the vendor or resource itself.

ELECTRONIC RESOURCE MANAGEMENT SYSTEM

An electronic resource management system, or ERMS, is powered by a knowledge base and is used to capture both electronic holdings and other e-resource-relevant acquisitions data. While librarians do not have the ability to directly modify the metadata contained within a knowledge base, they can use the ERMS to indicate which collections, packages, or individual resources their library subscribes to and the appropriate coverage dates for each one. For instance, a knowledge base may contain a collection of front file e-journals available for subscription from a publisher. A library may subscribe to only one of these journals, and only from the year 2015, which is when it first began its subscription. Through the ERMS, a librarian can select (or "track" or "activate") the single journal title from the collection and change its coverage dates to 2015–present in order to accurately represent the available access. The ERMS can also control other aspects of access and display, such as whether or not to include a proxy prefix for titles or collections, and the ability to include descriptions of access restrictions, such as seat or usage limitations. In other words, the knowledge base provides a reservoir of metadata from which a library can draw, but it is through an ERMS that the library indicates which metadata is relevant and adds additional information specific to their situation. Since edits cannot be made to the knowledge base itself but can be made to library selections, such as holdings and coverage dates, this knowledge management system has blended control.

Access disruptions originating from an ERMS, therefore, can be caused either by faulty metadata in the knowledge base, the symptoms of which we covered earlier, or from erroneously chosen holdings populated by a librarian. These could include

- incorrectly selected titles
- incorrect coverage dates
- missing proxy prefix
- erroneously added proxy prefix

These issues can result in library users encountering paywalls and proxy error messages or being unable to find accessible content within the library's discovery service.

LINK RESOLVER

Many ERMSs are sold with link resolver functionality, but link resolvers can also be sold as stand-alone products or in conjunction with other access tools, such as e-journal A–Z lists. Like ERMSs, link resolvers consist of a knowledge base containing e-resource and linking data and an administrative interface through which a library may select its holdings. These holdings are then used to populate access tools, such as e-journal A–Z lists and discovery services. As a result, access issues are caused either by faulty metadata within the knowledge base or by incorrect holdings chosen via the administrative interface. Symptoms would also be identical to those experienced by both a knowledge base and an ERMS, including broken or misdirecting links, paywalls, proxy error messages, and missing or erroneously included content.

CENTRAL INDEX

Missing, erroneous, and outdated metadata is also the primary cause of access issues originating from a central index. Like a knowledge base, a central index ingests metadata from hundreds of publishers and content providers, each of which has its own standards for representing e-resource metadata. This means the metadata quality often varies according to who is providing it and suffers from issues similar to those of a knowledge base regarding normalization, missing content, and lag time between when a resource is modified on a platform and when it is updated within the index. However, unlike a knowledge base, a central index is primarily used to provide discoverability for the contents comprising a larger work, such as articles, abstracts, book chapters, images, video segments, and so on. This distinction is important to remember because a knowledge base and a central index express similar symptoms—most typically, broken or misdirecting links—when their metadata is faulty, but the issue may need to be reported to a different vendor or support portal, depending on which company the library has contracted with for each. It is often easiest to identify whom to contact based on what type of discovery record is experiencing the problem.

Authentication

IP AND VPN AUTHENTICATION

IP address recognition has been the primary method of authentication to online library resources since the mid-1990s. For on-site users, the process is virtually invisible. They navigate to the e-resource while connecting to the internet via their institution's network (and thus IP address), and as long as the correct IP ranges have been registered with the vendor platform, the user is granted access without needing to log in or otherwise further identify themselves. However, off-site access using IP authentication has been more fraught. VPNs, for example, require users to download and utilize specialized software to make it appear as though their computer is on site. Even then, having navigated the installation process, users may still be denied access to content if the VPN is configured to utilize split tunneling, where only certain traffic is routed through the institution's IP ranges.

IP authentication is also susceptible to large-scale access disruptions. Any issues with an IP address will affect everyone utilizing that address, be it an individual user or an entire campus department building. An increasingly common example is unauthorized text and data mining. If a user engages in behavior that goes against a resource's licensing agreement, the vendor may choose to disable access to that resource to stop the behavior. Since authentication happens with the IP address, the vendor cannot block the individual user and is instead forced to disable access to the entire IP address. If that IP address is for the VPN or proxy, this block can adversely affect the access for everyone off site.

Errors also happen on the administration side. IP ranges may not be submitted to the vendor or entered into the platform to enable access. Also, IP ranges may change unexpectedly. As Dowling explains,

> Many of our institutions have, over the years, added additional campuses and additional networks, or have changed networks, requiring a continual need to revise the IP ranges we report to every one of our publishers. At the same time, the publishers have had to manage these continual changes from a growing number of institutions. The process has become time-consuming for everyone involved and increasingly prone to error. (Dowling 2020, 43)

PROXY AUTHENTICATION

Proxy servers can be either locally hosted by the library or remotely hosted by a vendor or other third-party entity, such as a consortium. Depending on where the proxy server is hosted, an institution may not be able to make direct edits to the server or its configuration files. Like all servers, proxy servers can experience downtime or lapses in access as a result of technical issues. They are also prone to the same IP authentication issues outlined earlier. However, proxies can also run into issues that revolve around the configuration files.

Library proxies require the maintenance of several configuration files in order to function, including one that contains the URLs, hosts, and domains of the e-resources licensed for IP authentication and access. These URLs, hosts, and domains are grouped by platform into entries called stanzas and need to be frequently updated in order to keep pace with changes to the platform. Access issues originating within this configuration file are generally the result of missing, erroneous, or incomplete stanzas and will result in users being confronted with a proxy error message or being forced to authenticate for open or free resources.

FEDERATED IDENTITY MANAGEMENT

Federated identity management is a more reliable and secure way to authenticate users compared to methods relying on institutional IPs. However, FIM authentication still has its challenges. Commonly identified access issues related to FIM authentication have to do with users finding and navigating the Where Are You From (WAYF) menu. While FIM-enabled platforms allow users to arrive at the content through any means, even through links from the wider web, users still need to identify which institution they are affiliated with when logging in. This is generally done using a WAYF menu, a drop-down menu that lists every available option. This list is potentially very long, and understandably users can encounter difficulty finding their correct institution if it is missing, confusingly labeled, or hard to find. Although improvements have been made to simplify the WAYF menu, including search features, a persistence service, and institutional naming standards, institutions still prefer to have users avoid the WAYF menu whenever possible. As a result, many institutions are using WAYFless URLs to bypass the menu entirely.

WAYFless URLs are specially formatted URLs that communicate the users' institutional affiliation to the service provider, thus redirecting the user to the appropriate log-in screen without having to select it from a list. WAYFless URLs are used primarily within institutional portals or discovery systems. Users navigating to the platform from the web would still need to use the WAYF menu. Also, depending on how the WAYFless URLs are constructed, they can be prone to breaking as a resource's web location information changes. This means a user may still be confronted with a WAYF menu even when using a WAYFless URL.

Finally, it is worth noting that not all vendor platforms support FIM, particularly smaller society publishers that may not have the staff bandwidth for implementation. Therefore, FIM is often utilized alongside other authentication methods in order to provide robust coverage. This can lead to additional confusion for users, who must maneuver through multiple authentication methods depending on the resource.

Vendor Platform

Access issues originating from a vendor platform fall into two categories: technology issues with the

Table 3.1. Common access issues and their solutions

Issue	Reason	Solution
User Error	The patron navigated to the resource from outside the library's access tools.	Educate the patron on how to access and use library e-resources.
	The patron incorrectly interpreted a library's holdings.	
	The patron is unfamiliar with using features of library e-resources.	
	The patron is attempting to access a resource from the wrong browser or without the necessary software.	
	The patron is no longer an authorized user.	
Vendor Cut Access	Your library does not have access to an e-resource due to a payment issue.	Work with the vendor and the library's acquisitions staff to process payment.
	The vendor incorrectly thought your library does not have access rights.	Contact the vendor to reestablish access on the platform.
Incorrect E-resource Implementation	Your library does not own or subscribe to the e-resource. You verify, via acquisitions or other records, that it should not have been made discoverable.	Remove the e-resource from discovery.
	Access was never established on the vendor platform when the e-resource was acquired.	Supply the vendor with the necessary information, such as IP addresses, to complete registration.
Broken or Misdirecting Link	Incorrect metadata in a link from research guide, ILS, or database A–Z list leads to an error message or being directed to the wrong content.	Navigate to the vendor platform to attempt to find the desired content elsewhere on its platform. Inform the patron of the alternate route. Change local records to reflect updates.
	Incorrect metadata in a link from knowledge base or central index leads to an error message or being directed to the wrong content.	Navigate to the vendor platform to attempt to find the desired content elsewhere on its platform. Inform the patron of the alternate route. Whether or not you find the content via an alternate route, contact the e-resource or access tool vendor to update its metadata.
	The e-resource URL is outdated due to a vendor website architecture change or content being removed.	Contact the vendor of either the access tool or e-resource to alert it of the outdated link with incorrect metadata.
	The e-resource record is used only for internal purposes and the access mechanism is not actively updated.	Suppress or otherwise hide the e-resource record from patron view.
Incorrect Holdings	Holdings do not accurately represent the library's access entitlements: • Incorrect coverage dates • Missing titles the library has subscribed to or purchased • Including titles not subscribed to or purchased by the library	Use acquisitions records, vendor title lists, or licenses, etc., to update your library's holdings within your access tools.
Authentication: EZproxy	An EZproxy prefix was not added to an e-resource's URL; patrons are therefore hitting a paywall.	Add the EZproxy prefix to the e-resource's URL.
	An EZproxy prefix was erroneously added to an e-resource's URL; patrons are receiving an EZproxy error.	Remove the EZproxy prefix to the e-resource's URL.
	The e-resource's stanza is not included in the EZproxy configuration file.	Add the EZproxy stanza to the EZproxy configuration file.
	The stanza for the e-resource in the configuration file is incorrect, e.g., missing host or domain name.	Correct the EZproxy stanza in the EZproxy configuration file.

Table 3.1 continued on page 20

Table 3.1. Common access issues and their solutions (cont.)

Issue	Reason	Solution
Authentication: VPN	Your institution's IT department has implemented split tunneling for your institution's VPN. The VPN is no longer routing e-resource traffic through the VPN.	Explain to patrons that the VPN no longer works as it used to and that they should not use it to access e-resources. In addition, work with your IT department and explain how the issue is confusing and an inconvenience to patrons and library staff. They may or may not choose to change how traffic is routed.
Authentication: FIM	Your institution's name is missing, confusingly labeled, or hard to find on the WAYF list on the e-resource's platform.	Contact the e-resource vendor to resolve this issue.
Authentication: Username/ Password	The patron has not created a necessary account with a particular e-resource and is attempting to log in with their library credentials.	Educate the patron on how to create the necessary account and to use it in the future to access the e-resource.
	A vendor has reset the username/password required for your library to access an e-resource without notifying your library.	Update the username/password for your patrons.
Unauthorized Text and Data Mining	A vendor has deliberately denied your library access to an e-resource due to unauthorized text and data mining.	Contact the patron to explain the situation and alert them of future requirements for compliance. Contact the vendor to tell them that you have notified the patron of their unauthorized use.

platform itself, such as the server being offline or the platform relying on old or obsolete technology, and deliberate denials of access by the vendor, usually due to a belief that the library no longer has rights to access the content. For technology issues, the symptoms are what you might expect to find with any website, such as slow loading times, error messages, and pages, scripts, or images not displaying correctly. These symptoms are reproducible and can be very widespread, affecting not just your library and users but also libraries and users from across the vendor's consumer base. They also require action on the part of the vendor in order to be resolved.

Fortunately, these platform issues are relatively rare and, issues with obsolete web technology aside, tend to be addressed quickly by the vendor. Instead, troubleshooters are much more likely to encounter deliberate denials of access. Acquisitions issues, such as missed invoices or incorrectly applied payments, are the most frequent reason a vendor would revoke access, but issues with content migration, excessive or suspicious usage and download activity (e.g., unauthorized scripting or text and data mining), and vendors updating their own websites or customer data sets can also cause deliberate access denials.

Common Access Issues and Their Solutions

In table 3.1, we have compiled some of the most commonly experienced access issues and their solutions. This list is not comprehensive but can act as a reference tool by briefly summarizing solutions to common problems encountered by troubleshooters.

References

Ashmore, Beth, Emily Allee, and Rebekah Wood. 2015. "Identifying and Troubleshooting Link-Resolution Issues with ILL Data." *Serials Review* 41, no. 1: 23–29. https://doi.org/10.1080/00987913.2014.1001506.

Ashmore, Beth, and David Macaulay. 2016. "Troubleshooting Electronic Resources with ILL Data." *Serials Librarian* 70, no. 1–4: 288–94. https://doi.org/10.1080/0361526X.2016.1153336.

Baskaran, Dharini. 2019. "Chat Ref Analysis—Exploring and Analyzing Chat Reference Transcripts Specifically Relating to Acquisitions and Discovery." *Serials Review* 45, no. 3: 132–36. https://doi.org/10.1080/00987913.2019.1647775.

Brett, Kelsey. 2018. "A Comparative Analysis of Electronic Resources Access Problems at Two University Libraries." *Journal of Electronic Resources Librarianship* 30, no. 4: 198–204. https://doi.org/10.1080/1941126X.2018.1521089.

Browning, Sommer. 2015. "Data, Data, Everywhere, nor Any Time to Think: DIY Analysis of E-resource Access Problems." *Journal of Electronic Resources Librarianship* 27, no. 1: 26–34. https://doi.org/10.1080/1941126X.2015.999521.

Crum, Janet A. 2011. "An Availability Study of Electronic Articles in an Academic Health Sciences Library." *Journal of the Medical Library Association* 99, no. 4 (October): 290–296. https://doi.org/10.3163/1536-5050.99.4.006.

Dowling, Thomas. 2020. "We Have Outgrown IP Authentication." *Journal of Electronic Resources*

Librarianship 32, no. 1: 39–46. https://doi.org/10.1080/1941126X.2019.1709738.

Enoch, Todd. 2018. "Tracking Down the Problem: The Development of a Web-Scale Discovery Troubleshooting Workflow." *Serials Librarian* 74, no. 1–4: 234–39. https://doi.org/10.1080/0361526X.2018.1427984.

Foster, Anita K. 2021. "A Controlled Vocabulary for an Electronic Resources Problem Reporting System: Creation, Implementation and Assessment." *Library Resources and Technical Services* 65, no. 1: 23–32. https://doi.org/10.5860/lrts.65n1.23-32.

Goldfinger, Rebecca Kemp, and Mark Hemhauser. 2016. "Looking for Trouble (Tickets): A Content Analysis of University of Maryland, College Park E-resource Access Problem Reports." *Serials Review* 42, no. 2: 84–97. https://doi.org/10.1080/00987913.2016.1179706.

Gould, Elyssa M., and Kelsey Brett. 2020. "A Tale of Two Universities: Electronic Resources Troubleshooting Comparisons." *Serials Librarian* 79, no. 1–2: 192–99. https://doi.org/10.1080/0361526X.2020.1760184.

Kimbrough, John. 2018. "Technical Services and the Virtual Reference Desk: Mining Chat Transcripts for Improved E-resource Management." *Serials Librarian* 74, no. 1–4: 212–16. https://doi.org/10.1080/0361526X.2018.1428482.

Lounsberry, Megan, Nicole Wood, and Bonnie Thornton. 2021. "The Power of Cross-Unit Data Sharing: Nontraditional Uses for ILLiad." *Serials Librarian* 80, no. 1–4: 131–34. https://doi.org/10.1080/0361526X.2021.1879759.

Lowry, Lindsey. 2020. "Where Do Our Problems Lie? Comparing Rates of E-access Problems across Three Research Institutions." *Serials Review* 46, no. 1: 26–36. https://doi.org/10.1080/00987913.2020.1733173.

———. 2021a. "Exploring the Evidence-Base for Electronic Access Troubleshooting: Where Research Meets Practice." *Journal of Electronic Resources Librarianship* 33, no. 3: 156–69. https://doi.org/10.1080/1941126X.2021.1949153.

———. 2021b. "Fighting an Uphill Battle: Troubleshooting Assessment Practices in Academic Libraries." *Library Resources and Technical Services* 65, no. 1: 4–13. https://doi.org/10.5860/lrts.65n1.4-13.

Mann, Sanjeet. 2015. "Electronic Resource Availability Studies: An Effective Way to Discover Access Errors." *Evidence Based Library and Information Practice* 10, no. 3: 30–49. https://doi.org/10.18438/B88C82.

Mann, Sanjeet, and Sarah Sutton. 2015. "Why Can't Students Get the Sources They Need? Results from a Real Electronic Resources Availability Study." *Serials Librarian* 68, no. 1–4: 180–90. https://doi.org/10.1080/0361526X.2015.1017419.

Nisonger, Thomas E. 2009. "A Simulated Electronic Availability Study of Serial Articles through a University Library Web Page." *College and Research Libraries* 70, no. 5 (September): 422–445. https://doi.org/10.5860/0700422.

Wright, Jennifer. 2015. "Electronic Outages: Who Broke It? How Long Was It Broken? We're . . . Tracking That, Right? Report from ALA Midwinter 2015." *NASIG Newsletter* 30, no. 2. https://tigerprints.clemson.edu/cgi/viewcontent.cgi?article=1662&context=nasig.

Methods of Diagnosis

Troubleshooting efforts are divided into two types: reactive and proactive. Reactive troubleshooting is efforts to diagnose and resolve reports of e-resource access disruptions received by libraries. These efforts are not planned, but in response to a previously unknown need. Conversely, proactive troubleshooting represents efforts that attempt to mitigate the daily influx of problem reports by identifying and resolving issues ahead of time. Unfortunately, many libraries are unable to dedicate a significant number of staff to engage in reactive troubleshooting. Proactive efforts, too, are often neglected due to a scarcity of staffing resources. As Rathmel and colleagues (2015) conclude from the results of their troubleshooting survey: out of 234 library respondents, 67 percent reported primarily troubleshooting with reactive approaches, and only 27 percent reported proactively troubleshooting. Consequently, libraries are looking for tools to diagnose and resolve access issues as efficiently as possible.

One of the significant gaps in library troubleshooting literature is methods of diagnosis. This is understandable given that each library system and electronic collection is unique. Both Rathmel and colleagues (2015) and Heaton (2018) ask the question "What are the best tools for troubleshooting?" Much of their focus is on tools that gather information, communicate resource status, and coordinate tasks. These include e-mail programs, ticket trackers and customer relationship management (CRM) systems, intranet applications, ERMSs, and project management platforms. While these tools are important for troubleshooting, forming the backbone of data collection and communication, they do not represent the best tools for diagnosing, which many novice troubleshooters seek. In this chapter, we attempt to fill this gap by reviewing trends and common methods of diagnosis for both reactive and proactive troubleshooting discussed in the literature and presented at conferences or workshops.

Troubleshooting Methodology: A Modified Version of Ross and Orr's DECSAR

Several troubleshooting methodologies already exist within the discipline of information technology, including the six-step methodology recommended by the Computing Technology Industry Association (CompTIA) and the DECSAR method, which was first developed by Ross and Orr (2009) to assist in the education and training of novice troubleshooters. We recommend a modified version of Ross and Orr's DECSAR method in our book *The Electronic Resources Troubleshooting Guide* (Talbott and Zmau 2020). It specifically addresses the library troubleshooting needs around communication, assessment, and documentation and consists of these seven stages:

1. Identify and define the problem.
2. Examine the situation.
3. Consider the possible causes.
4. Consider the possible solutions.
5. Implement the solution.
6. Review the results.
7. Communicate and document the resolution.

When compared to other troubleshooting methodologies, the DECSAR method in particular is notable for its depiction of the iterative nature of troubleshooting. This method identifies both the ideal linear path, which is often the sole focus of other troubleshooting methodologies, and the backtracking, or recursive thinking, that is necessary depending on the complexity of the issue and the skill of a troubleshooter. As we discuss reactive and proactive troubleshooting efforts throughout this chapter, we will concern ourselves with step number 3 of our DECSAR troubleshooting method and consider the possible causes.

Reactive Troubleshooting

Techniques for Diagnosis

Troubleshooting diagnosis can be overwhelming. As Emery, Stone, and McCracken (2020) explain, when attempting to diagnose an access disruption, "it is impractical to check all of the following variables, and especially to check all variables against all other variables" (97). When confronted with all the possible variables to check, novice troubleshooters often do not know where or how to begin. Along with the DECSAR method, the following techniques can be used by troubleshooters to jump-start their diagnosis:

- *Re-creation:* The troubleshooter isolates the cause of the issue by finding a procedure (sequence of steps or events) that consistently induces the symptoms or failure to occur.
- *Elimination:* The troubleshooter isolates the cause of the issue by systematically testing and eliminating possible causes.
- *Backtracking:* The troubleshooter isolates the cause of the issue by starting at the point of system failure and reasoning backward, testing each possible cause along the way (Gugerty 2007).
- *Half-splitting:* Using this method, the troubleshooter divides the system into portions and checks each portion for symptoms of the issue; this procedure is repeated in the portion where the symptoms occur (by again dividing and testing each half) until the cause of the issue has been isolated.

Re-creation is perhaps the most widely employed and talked about method for e-resource troubleshooting. In their book *The ABCs of ERM*, Zellers, Adams, and Hill list it as the first step in their four-part troubleshooting process, and also one that frontline staff should be trained to do before transferring problems to the specialists (Zellers, Adams, and Hill 2018, 158). Other articles, including Davis and colleagues (2012), Browning (2015), Hart and Sugarman (2016), and Shriver (2019), also mention this method, usually couched within the context of tools meant to facilitate the re-creation process. By attempting to replicate an issue, the troubleshooter gains essential contextual information that verbal or written descriptions simply cannot provide. Often, this information is enough to pinpoint the cause of the access issue without the need for additional testing or investigation. Therefore, the very first troubleshooting strategy we recommend that all troubleshooters try when diagnosing an access issue is re-creation.

For instance, whether the source of an access issue is within a patron-controlled component (e.g., device, browser, or internet connection) or within a library- or vendor-controlled component (e.g., catalog, knowledge base, discovery service) will affect whether the troubleshooter is able to reproduce the issue.

As a general rule of thumb, reproducible problems indicate that the cause of the breakdown is within the library-controlled or vendor-controlled part of the access chain. This makes sense, of course. If an issue is presenting itself to multiple users (in this case, the reporter and the troubleshooter) who are employing different devices, browsers, and network settings, the issue is likely unrelated to these patron-specific components. There are exceptions to this rule, of course, mostly in regard to browsers and browser settings, which can be reproduced if the troubleshooter is given enough information.

Elimination is another method frequently discussed in the literature, although usually without naming it as such. The suggested strategies usually entail testing certain components, such as browsers, caches and cookies, or devices, by replacing or removing them from the access chain to see if the issue reappears. This could mean asking patrons to use a different device or browser, to clear their browser's cache and cookies, to disable any advertising or pop-up blockers, or to modify their security settings. This also means being aware of any compatibility issues or software requirements for specific vendor platforms. If a vendor platform is not compatible with mobile devices or can be accessed using only certain browser versions or DRM software, the troubleshooter should first check that the patron is meeting these requirements before diving into additional problem solving. For instance, Emory, Stone, and McCracken developed a browser rubric to systematically test popular browsers on Macs and PCs from both on and off site (Emory, Stone, and McCracken 2020, 103). By diligently testing each combination, a troubleshooter can gain a comprehensive view of which factors—browser, device, location, or a combination—contribute to the appearance of the access failure.

Both re-creation and elimination are extremely useful in isolation; however, they alone cannot solve every issue. Sometimes, they will need to be used in conjunction with other troubleshooting methods to pinpoint the cause of an access disruption. Consider this example of backtracking: a troubleshooter receives a problem report from a professor who cannot access an e-resource from within the learning management system (LMS). Through the troubleshooting interview, the troubleshooter learns that the professor had embedded one of the library's research guides within a course page, but when the professor clicked on the link to a database included in the guide, he received a 404 error message. Presuming the troubleshooter has access to the course page, the troubleshooter would first attempt to replicate the issue by navigating to the embedded guide and clicking the link. (Alternatively, the troubleshooter could navigate directly to the research guide from the library website to test the link there.) The troubleshooter receives the same 404 error message. After taking a closer look at the link, the troubleshooter discovers it is a friendly URL originating from the library's database A–Z list. The troubleshooter then navigates to the database A–Z list and tests that link. It, too, produces a 404 error message. Logging into the back end of the A–Z list, the troubleshooter compares the entry's URL (the one masked by the friendly URL) to that currently being used on the database's home page. The URLs are different. The troubleshooter updates the database entry to use the current home page URL, which resolves the issue and allows the professor to access the database from within the LMS.

While re-creating the issue was an essential first step in diagnosis, replication alone was insufficient to pinpoint the cause. Because the URL of the link was passed through three access tools (database A–Z list to research guide to LMS course page) as well as hidden behind a friendly URL, simply finding and testing the link revealed very little as to why it was broken. Instead, the troubleshooter needed to follow the data back to its original source, testing along the way. This process of moving from LMS to research guide to database A–Z list is a great example of backtracking, which is most useful when trying to trace the origins of faulty metadata.

Half-splitting (also called chunking or the divide-and-conquer method) is another useful strategy for isolating the cause of an access issue. Using this method, the troubleshooter divides a system into segments (traditionally, into halves, thus the term *half-splitting*) and tests each segment for signs of the problem, repeating the process of dividing and testing until the faulty component is identified. Half-splitting is most effective when the troubleshooter is uncertain which area of the access chain an issue is originating from and wants to systematically test each portion, rather than randomly testing or eliminating components.

For instance, let's imagine a troubleshooter is trying to determine why an off-campus patron is receiving a timeout error message when accessing an e-resource via the library's e-journal A–Z list. The troubleshooter could mentally divide the access chain into two halves: the patron-controlled components and authentication in one half and the e-journal A–Z list and vendor platform in another. To test the first half, the troubleshooter could provide the patron with a proxied link to a test e-resource—one the troubleshooter knows works correctly—and ask the patron to attempt to access the content. To test the second half, the troubleshooter navigates to the faulty e-journal within the A–Z list and attempts to access it firsthand. The troubleshooter is successfully able to view the journal on the vendor platform, but the patron reports that using the test link caused the timeout error message to appear.

Since the issue appeared again for the patron but not the troubleshooter, the next step would be to divide the first segment into its distinct pieces to test authentication and the patron-controlled components separately. To test the authentication, the troubleshooter could ask the patron to attempt to access an e-resource using the WAYF menu on a federated SSO-enabled vendor platform. This bypasses the proxy server entirely, while allowing the patron to use the same device, browser, and network connection as before. To test the device, browser, and network connection, the troubleshooter could first ask whether the patron has experienced connection issues, such as slow load times, while using nonlibrary web resources. The troubleshooter may also have the patron assess personal connection speed using a free online tool. However, the troubleshooter would likely want to wait for the results of the WAYF test before diving too far into such tests.

The patron reports being able to access the content using the WAYF menu and having no connection issues while browsing the web. This implies that some negative interaction with the proxy server (i.e., authentication) is at fault. Based on experience, the troubleshooter knows that browser cookies often interact negatively with the proxy server, so the troubleshooter would likely ask the patron to clear the cache and cookies as well as browsing history or attempt to use another browser entirely to see if either resolves the issue. If the issue persists or if more patrons report similar errors, the troubleshooter may want to consult with the staff who manage the proxy server in order to come to a satisfactory resolution, such as modifying the configurations or updating the server software.

Again, in this example, re-creation by itself was of limited value to the troubleshooter. Since the issue appeared for the patron but not the troubleshooter, it was difficult for the troubleshooter to gauge which components were contributing to the issue and which were extraneous. Similarly, while elimination may have eventually isolated the cause of the error, testing individual components in a sequential order—or, worse, jumping between components randomly or whenever inspiration strikes—is inefficient and can lead to frustration as time drags on. By chunking the access chain into segments and systematically testing each one, the troubleshooter was able to quickly home in on the culprit.

Tools for Diagnosis

GENERIC TOOLS

What's My IP

Knowing the exact IP address for an end user's computer can be helpful to quickly determine if they are located on or off site. Similarly, troubleshooters often provide their IP address to vendors to help troubleshoot systemic issues. An originating IP address can be determined by querying Google "What's my IP?" or by visiting websites such as WhatIsMyIPAddress.

WhatIsMyIPAddress
https://whatismyipaddress.com

Incognito Mode

Troubleshooters can use incognito mode to test whether a browser's cache, cookies, or browsing history is interfering with access. This feature is referred to as Incognito Mode in Chrome, Private Browsing in Firefox, InPrivate Browsing in Microsoft Edge, and Private Window in Safari. Incognito mode works by creating a separate, "clean" session within a browser, free from any previously stored web data. This allows troubleshooters to effectively clear their caches and cookies without actually losing any of the information.

Verifying If a Website Is Down

There are several websites that can verify if a web page is down for just your PC (personal computer) or for everyone. These websites allow you to plug in a URL to see how many users are affected by a vendor's potential downtime.

Downforeveryoneorjustme.com
https://www.downforeveryoneorjustme.com

IsItDownRightNow?
https://www.isitdownrightnow.com

Solutions Repository

Some libraries have found success by implementing local solutions repositories to address regular troubleshooting issues. A solutions repository can take the form of a blog, wiki, Word document, research guide, and so on. Its purpose is to proactively list solutions to common, simple, or known issues so that troubleshooters can respond more quickly to access issues. Some commercial ticketing systems have features similar to a solutions repository. For example, Springshare's LibAnswers provides an option to reuse previous ticket answers called Reuse Answers. Examples for what to incorporate into a solutions repository include e-resources that often confuse users, tricky technology configurations, e-resources that require individual accounts for access, and e-resources or vendors known for lengthy downtimes.

A solutions repository can be useful both for troubleshooting staff and for other staff whose primary duties may not include troubleshooting. As Samples and Healy highlight, "Public-facing staff can do access problem triage by consulting the wiki and getting back to the patron with an explanation without having to submit a form or an email to the troubleshooting team" (Samples and Healy 2014, 114).

Screen Capturing Programs

Screen capturing programs like Snipping Tool (Windows), TechSmith Capture, or Snagit (TechSmith) are frequently mentioned throughout the literature and can be invaluable for troubleshooters who struggle to see exactly what their reporters are reporting. By requesting a screenshot from a user, a troubleshooter can identify pertinent details from the image, such as if the user's browser URL field includes proxy details or if the user is appropriately signed in to an e-resource with their account. Troubleshooters also use screenshots to communicate more easily with vendors and to capture detailed instructions for users that would otherwise be cumbersome to communicate via e-mail.

TOOLS FOR TROUBLESHOOTING OPENURL LINK RESOLVER ISSUES

Carter and Traill facilitated a workshop called Teaching Troubleshooting at the 2019 Electronic Resources and Libraries Conference in Austin, Texas. The workbook they provided for the workshop includes a list of practical diagnosing tools such as extensions for HTTP headers, options for parsing OpenURLs, and local bookmarklets for revealing discovery service source records (Carter and Traill 2019). These tools are highly relevant and practical for troubleshooting OpenURL issues.

Parsing OpenURLs into their individual components can make them more easily readable, aiding in identifying faulty metadata for quicker resolution. Carter and Traill (2019) specifically mention Jeff Peterson's OpenURL deconstructor (Peterson, n.d.) and the FreeFormatter URL Parser/Query String Splitter (FreeFormatter, n.d.). These tools can be used to determine if incorrect metadata is causing an OpenURL link to fail. Relatedly, various browser extensions can be employed to view the HTTP headers in a browser. HTTP headers display the header name and value, often separated by a single colon, for both HTTP requests and responses. For troubleshooting, viewing HTTP headers can reveal the exact requests and responses that are being processed in real time when attempting to access an e-resource. This in turn can aid in spotting if proxy details are being appropriately passed or where exactly a connection is being lost when a link fails.

Some libraries have developed their own tools that can be used to troubleshoot common issues within their local systems. Carter and Traill (2019) specifically mention that bookmarklets are beneficial for troubleshooting their local system Ex Libris's Alma LSP. A bookmarklet is a web browser bookmark that contains JavaScript commands that add new features to the browser. Ex Libris provides a Developer Network for its customers where information and technology solutions can be shared in benevolence among the Alma community. For example, the bookmarklet PrimoNUIShow is used to display the RecordID and PNX source record for a record from the Primo discovery search (Höfler 2018). The PNX record can be very useful when troubleshooting Primo discovery search issues because it reveals the source of the original record and therefore reveals who should be contacted, be it the vendor, Ex Libris, or the local library, when an issue is encountered.

TOOLS FOR TROUBLESHOOTING REMOTE ACCESS

The cornerstone for troubleshooting remote access is simulating off-site access while being on site. This is usually done by utilizing on-site technology with an IP address not included in the institution's on-site ranges. There are several different technology options to achieve this goal. Rodriguez, Tonyan, and Wilson (2018) include a list of practical diagnosing tools for troubleshooting remote access, such as smartphones connected to a cellular network, mobile Wi-Fi hotspots, remote desktop solutions, commercial (not institutional) VPNs, and advanced troubleshooting options for EZproxy. We review a few of these tools here.

Smartphones connected to a cellular network are often a first stop for troubleshooters looking to troubleshoot remote access; however, there are downsides to this. Using a personal device for work purposes is an imperfect solution, and a strong cellular network connection is required. Depending on the volume of troubleshooting needed and the library staff member's data plan, data costs may be significant. Moreover, access disruptions may pertain to specific devices or operating systems that are unable to be tested on a smartphone.

Personal devices can also be used for troubleshooting when connected to mobile Wi-Fi hotspots. Mobile hotspots are considered affordable both for initial purchase cost and annual data rates, and they can be especially handy for troubleshooters whose libraries already offer hotspot devices for checkout to their users. However, some institutions may restrict work machines from logging on to external wireless networks.

Beyond a smartphone or mobile Wi-Fi hotspot, remote desktop solutions are another common option. Remote desktop solutions, such as Microsoft Remote Desktop, TeamViewer, and Chrome Remote Desktop, allow a desktop to be controlled from another computer or device (Rodriguez, Tonyan, and Wilson 2018). External VPNs are also a very popular troubleshooting solution; however, some commercial VPNs are subject to increased scrutiny from institutional IT departments, which may or may not restrict staff from being able to download and install the commercial VPN client on the internal network.

Several resources exist for troubleshooting remote user access issues originating from the institution's proxy server. They include access to the local configuration files, OCLC's EZproxy Database Stanzas list, the EZproxy LISTSERV, and configuration file directives that can be used by EZproxy administrators. Many proxy issues can be resolved by updates to the e-resource's stanza within the configuration file. With access to the local configuration file, troubleshooters can swiftly enact these updates. OCLC manages a list of current stanzas on its EZproxy Database Stanzas list. Troubleshooters can use this list to verify what the most current stanza for an e-resource platform should be. The OCLC EZproxy Database Stanzas list should be the first place troubleshooters check after verifying a proxy prefix has been applied appropriately to a resource URL. E-resource platform vendors are also able to provide stanzas for their products upon request. Additionally, the EZproxy LISTSERV is an invaluable resource for being proactively notified of proxy issues with major vendors. The LISTSERV also provides an outlet for discussion and the opportunity to learn how to better resolve issues from other, more seasoned professionals. Finally, the EZproxy RequireAuthenticate and MinProxy directives can be used for simulating remote access. More information about these directives can be found in OCLC's online support portal.

Proactive Troubleshooting

One of the avenues for attempting to reduce the number of problem reports received is to analyze problem reports to identify systemic issues. Another is to conduct routine access checks for a library's holdings. Both of these proactive methods can be helpful in reducing both user and librarian frustration. Analyzing problem reports can reveal a library's most common issues, uncover previously unknown underlying issues, and help a troubleshooting team determine where they can correct their course to better invest their limited resources. Conducting routine access checks can discover broken links before users are able to report them. Proactive troubleshooting also encompasses working with access tool or e-resource vendors to address known issues via the vendor website, e-mail, phone, or in-person communication, as well as working with peer librarians whose libraries use similar products.

Analyzing Problem Reports

Analyzing problem reports can directly tie in to workflow assessment because so many different variables can be evaluated against initial assumptions or preconceived notions. Many libraries choose to analyze their problem reports with these goals in mind (Lowry 2021):

- to identify common points of failure
- to identify any underlying, systemic issues with particular e-resources, authentication methods, access tools, or user groups
- to determine if additional staffing resources are needed due to ticket volume
- to identify gaps in the troubleshooting workflow
- to inform collection development decisions
- for training purposes

There is much discussion in the literature concerning the need for a controlled vocabulary when analyzing problem reports. Individual libraries can analyze their own tickets using their own terms and categorization methods. However, in order for an individual library to gain context for the results of its local analysis, a shared language of description would be necessary. Gould and Brett (2020) note that currently further standardization and agreed-upon definitions would be required to see the true value in a shared vocabulary. Both Gould and Brett (2020) and Goldfinger and Hemhauser (2016) propose that a NISO standard be created for categorizing e-resource access issues. As Gould and Brett state, "Developing a NISO standard would be the best way to codify Goldfinger and Hemhauser's problem types and functional areas and lead to wide adoption within the library community" (Gould and Brett 2020, 198). Some libraries are adopting the controlled vocabulary, called "Functional Areas," developed by Goldfinger and Hemhauser (2016). Examples of Goldfinger and Hemhauser's Functional Areas include KB/link resolver, proxy/IP problems, incorrect URL, excessive usage/downloading, and subscription problem.

Brett (2018) used Goldfinger and Hemhauser's (2016) controlled vocabulary, and Lowry (2020) then built upon the work of Goldfinger and Hemhauser (2016) and Brett (2018) in her own ticket analysis in order to identify trends that could signal an industry-wide issue. The study confirmed that "certain types of access problems do occur at similar rates among research institutions, despite the likely differences in workflows, tools, management styles, and varying collections among them" with the "two most common problems at all three libraries f[alling] into the categories of KB/Link Resolver or Platform" (Lowry 2020, 29). To supplement this analysis, Lowry also created a locally defined schema to illuminate access disruption trends affecting her institution. Example categories include concurrent user limits, bad record in catalog, DDA problem, referral to another department, and accessing canceled titles/resources.

Access Checks

As libraries subscribe to or purchase e-resources, a record is usually created to serve as a receipt for what the library is gaining access to and for how long. These receipts usually take the form of title lists from licenses, subscription agent interfaces, or vendor administration portals. Acquisition records can also provide more details. Title lists from these sources usually include a title, a unique identifier (such as ISBN or ISSN), publisher or vendor information, coverage dates, and the website where the licensed content can be accessed. Subscription coverage dates vary widely from vendor to vendor, and libraries have not always licensed perpetual access to content they pay for. To determine whether the library retains perpetual access or post-cancellation access, a troubleshooter would need to consult the resource's specific license terms.

Although librarians do their best when making e-resources available for discovery, inaccuracies inevitably occur in a library's holdings long after the e-resources were originally acquired. Especially for e-journals, which can experience changes in title, publisher, and hosting provider, the very nature of subscriptions introduces variables that can cause a library's access to be inadvertently cut off. A vendor, for example, may accidentally disable a library's access even after a renewal invoice is paid or may fail to reestablish access after receiving a late payment. One-time purchases can also experience similar acquisitions issues due to continuing access fees.

In response to these issues, some libraries perform systematic access checks with the goal of comparing a reliable access list, such as a vendor title list, to what has already been enabled within the library's discovery system. An access check for a single subscription ensures that the correct title, coverage dates, and platform for access are available for users to discover. A vendor title list can be cross-referenced with acquisitions data when available, and acquisitions data alone can be used if a vendor does not provide a title list of subscriptions or one-time purchases.

Mortimore and Minihan (2018) go into great detail about how often they conduct access checks for various types of e-resources and why. Their troubleshooting staff perform bi-weekly database link audits and quarterly link asset audits and have a rolling link resolver audit. When prioritizing where to start when beginning e-resource access checks, many libraries consider the following:

- Any known, systemic issues: For example, a library has received multiple problem reports that it is missing access to titles on a single e-journal platform. Until the troubleshooter obtains a title list for the vendor platform, the troubleshooter will be unable to correct these issues en masse.
- A library's major vendors: For example, if the vast majority of a library's holdings are held between five to six vendors, it would be best to start with them.
- A library's most popular resources: Prioritize by subject discipline, audience size, or highest usage.
- Any obvious discrepancies in what a library should have access to and what a library cataloged: If a title list retrieved from a publisher states that a library should have access to twenty titles but instead the library has fifty titles cataloged, this should likely be examined sooner rather than later.

Spot-checking is also an alternative if a library does not have the staff time to devote to checking title lists, and so on, in their entirety. With limited staff time, a troubleshooter could check 20 percent of a library's holdings to determine if checking the remaining 80 percent is warranted. Not all title lists need to be checked individually in their entirety. It can also be argued that single title subscriptions that are dynamic by nature, such as e-journals and e-book packages, should probably be checked more frequently than one-time purchases that are static by nature, such as databases, e-books, and streaming videos.

Another remedy for limited staff time is to take advantage of any available link-checking features offered by access tools. For example, Springshare offers an automated link-checking tool that libraries can use to find broken links in both LibGuides and LibGuides A–Z Database List. There are also other link-checking tools that you may be able to use at your library, such as Callisto (Headlee and Lahtinen 2014; Sharp Moon 2017) or SEESAU (Serials Experimental Electronic Subscription Access Utilities; Collins and Murray 2009). In addition, it is common for libraries to use homegrown link checkers, often utilizing Python programming language, that are developed either by IT departments or by troubleshooting librarians who are familiar with coding.

Even without link-checking tools, access checks can be conducted periodically by a staff member. Access checks are usually simple enough that they can be assigned to student workers or to any other staff members who are unfamiliar with e-resources. Generally, once shown the basic requirements of link-checking, these staff members will succeed.

References

Brett, Kelsey. 2018. "A Comparative Analysis of Electronic Resources Access Problems at Two University Libraries." *Journal of Electronic Resources Librarianship* 30, no. 4: 198–204. https://doi.org/10.1080/1941126X.2018.1521089.

Browning, Sommer. 2015. "Data, Data, Everywhere, nor Any Time to Think: DIY Analysis of E-resource Access Problems." *Journal of Electronic Resources Librarianship* 27, no. 1: 26–34. https://doi.org/10.1080/1941126X.2015.999521.

Carter, Sunshine, and Stacie Traill. 2019. "Teach Your Staff to Troubleshoot E-resources: Practical Processes for Documenting and Implementing a Troubleshooting Training Curriculum." Workshop presented at the 2019 Electronic Resources & Libraries Conference, Austin, TX, March 6, 2019.

Collins, Maria, and William T. Murray. 2009. "SEESAU: University of Georgia's Electronic Journal Verification System." *Serials Review* 35, no. 2: 80–87. https://doi.org/10.1080/00987913.2009.10765216.

Davis, Susan, Teresa Malinowski, Eve Davis, Dustin MacIver, Tina Currado, and Lisa Spagnolo. 2012. "Who Ya Gonna Call? Troubleshooting Strategies for E-resources Access Problems." *Serials Librarian* 62, no. 1–4: 24–32. https://doi.org/10.1080/0361526X.2012.652459.

Emery, Jill, Graham Stone, and Peter McCracken. 2020. *Techniques for Electronic Resource Management: TERMS and the Transition to Open*. Chicago: ALA Editions. https://pdxscholar.library.pdx.edu/cgi/viewcontent.cgi?article=1305&context=ulib_fac.

FreeFormatter. n.d. "URL Parser/Query String Splitter." https://www.freeformatter.com/url-parser-query-string-splitter.html.

Gugerty, Leo. 2007. "Cognitive Components of Troubleshooting Strategies." *Thinking and Reasoning* 13, no. 2: 134–63. https://psycnet.apa.org/doi/10.1080/13546780600750641.

Goldfinger, Rebecca Kemp, and Mark Hemhauser. 2016. "Looking for Trouble (Tickets): A Content Analysis of University of Maryland, College Park E-resource Access Problem Reports." *Serials Review* 42, no. 2: 84–97. https://doi.org/10.1080/00987913.2016.1179706.

Gould, Elyssa M., and Kelsey Brett. 2020. "A Tale of Two Universities: Electronic Resources Troubleshooting Comparisons." *Serials Librarian* 79, no. 1–2: 192–99. https://doi.org/10.1080/0361526X.2020.1760184.

Hart, Katherine A., and Tammy S. Sugarman. 2016. "Developing an Interdepartmental Training Program for E-resources Troubleshooting." *Serials Librarian* 71, no. 1: 25–38. https://doi.org/10.1080/0361526X.2016.1169569.

Headlee, Patricia A., and Sandra C. Lahtinen. 2014. "Callisto Basic and Calisto Pro." *Journal of the Medical Library Association* 102, no. 4 (October): 305–6. https://doi.org/10.3163%2F1536-5050.102.4.018.

Heaton, Robert. 2018. "Tools for Troubleshooting: Which Ones and What For." *Journal of Electronic Resources Librarianship* 30, no. 1: 9–26. https://doi.org/10.1080/1941126X.2018.1443903.

Höfler, Gabriele. 2018. "New UI Bookmarklet: Show RecordID, PNX, Source Record." *Tech Blog*, March 22, 2017; updated December 18, 2018. Ex Libris Group. https://developers.exlibrisgroup.com/blog/New-UI-Bookmarklet-Show-RecordID-PNX-Source-Record/.

Lowry, Lindsey. 2020. "Where Do Our Problems Lie? Comparing Rates of E-access Problems across Three Research Institutions." *Serials Review* 46, no. 1: 26–36. https://doi.org/10.1080/00987913.2020.1733173.

———. 2021. "Fighting an Uphill Battle: Troubleshooting Assessment Practices in Academic Libraries." *Library Resources and Technical Services* 65, no. 1: 4–13. https://doi.org/10.5860/lrts.65n1.4-13.

Mortimore, Jeffrey M., and Jessica M. Minihan. 2018. "Essential Audits for Proactive Electronic Resources Troubleshooting and Support." *Library Hi Tech News* 35, no. 1: 6–10. https://doi.org/10.1108/LHTN-11-2017-0085.

Peterson, Jeff. n.d. "OpenURL Parser." https://gpeterso.github.io/url-params/.

Rathmel, Angela, Liisa Mobley, Buddy Pennington, and Adam Chandler. 2015. "Tools, Techniques, and Training: Results of an E-resources Troubleshooting Survey." *Journal of Electronic Resources Librarianship* 27, no. 2: 88–107. https://doi.org/10.1080/1941126X.2015.1029398.

Rodriguez, Michael, Joel Tonyan, and Robert T. Wilson. 2018. "Tools and Techniques for Troubleshooting Remote Access." *Journal of Electronic Resources Librarianship* 30, no. 3: 171–78. https://doi.org/10.1080/1941126X.2018.1494095.

Ross, Craig, and R. Robert Orr. 2009. "Teaching Structured Troubleshooting: Integrating a Standard Methodology into an Information Technology Program." *Educational Technology Research and Development* 57, no. 2: 251–65. https://doi.org/10.1007/s11423-007-9047-4.

Samples, Jacquie, and Ciara Healy. 2014. "Making It Look Easy: Maintaining the Magic of Access." *Serials Review* 40, no. 2: 105–17. https://doi.org/10.1080/00987913.2014.929483.

Sharp Moon. 2017. "Callisto." https://sharpmoon.com/callisto/.

Shriver, Emery. 2019. "Managing Discovery Problems with User Experience in Mind." *Code4Lib Journal*, no. 44 (May). https://journal.code4lib.org/articles/14481.

Talbott, Holly, and Ashley Zmau. 2020. *The Electronic Resources Troubleshooting Guide*. Chicago: ALA Editions.

Zellers, Jessica, Tina M. Adams, and Katherine Hill. 2018. "I Think the Internet Broke." In *The ABCs of ERM: Demystifying Resource Management for Public and Academic Librarians*, 154–168. Santa Barbara, CA: Libraries Unlimited.

Current Initiatives Aimed at Mitigating Access Issues

Metadata Initiatives

Faulty and incomplete metadata is one of the primary culprits of e-resources access disruptions. In response, the National Information Standards Organization (NISO) has launched several initiatives to standardize the way e-resource metadata is represented and transmitted between organizations. We discuss a few of those initiatives in this section.

Knowledge Bases and Related Tools (KBART)

The NISO Knowledge Bases and Related Tools Recommended Practice (NISO RP-9-2010) was originally created in 2010 to address the myriad metadata problems associated with OpenURL linking failure (NISO, n.d.). The recommended practice focused on standardizing the e-journal metadata elements that needed to be communicated from content providers to the link resolver/knowledge base vendor in order to make the link resolver work. It also established the methods and frequency by which these metadata elements should be transmitted. However, as the role of knowledge bases within the discovery landscape grew, the scope of KBART expanded to tackle e-resource metadata issues beyond OpenURL. In 2014, KBART was updated to include standardized metadata elements for consortia, open-access publications, e-books, and conference proceedings (NISO RP-9-2014) (KBART Phase II Working Group 2014). And in 2019, the KBART standing committee introduced a proposal for Phase III that would expand the standardized metadata elements to include additional e-resources content types, such as audio, video, and data sets, as well as metadata for more granular items, such as article and chapter level entitlements.

While the KBART recommended practice is regarded as a successful endeavor in and of itself, helping to improve the quality of knowledge bases and thus discovery services industry-wide, its related recommended practice—KBART Automation—may prove even more instrumental in mitigating access disruptions. Adopted in 2019, the KBART Automation recommended practice (NISO RP-26-2019) utilizes the KBART format to enable content providers to send institution-specific holdings reports to that institution's knowledge base via an automated API process, thus allowing "knowledge base-powered systems to more accurately reflect content accessible at a particular institution and its unique holdings, with little interaction or ongoing maintenance from library staff" (KBART Automation Working Group 2019, v). Not only does this more direct communication have the potential to reduce the amount of time library staff spend monitoring and maintaining access entitlements in the knowledge base, it may also reduce the number of errors introduced during the maintenance process. In turn, end users are less likely to run into paywalls or denials of access due to incorrect knowledge base selections.

However, KBART Automation does come with a few downsides. Without the need for manual maintenance, librarians may become less aware of what updates are being made to the knowledge base on their behalf. As Derouchie, Ashmore, and Van Gorden point out, "Librarians would have fewer opportunities to review and identify any discrepancies in data. New workflows may need to be implemented to allow the librarian to detect and resolve these discrepancies" (Derouchie, Ashmore, and Van Gorden 2021, 120). Furthermore, automated holdings may allow for less customization and choice over the content being activated in the knowledge base, such as with promotional or time-limited offers of free content.

Open Discovery Initiative (ODI)

The Open Discovery Initiative (NISO RP-19-2020) was initiated in 2011 to establish a set of recommended best practices for index-based discovery services (Open Discovery Initiative Standing Committ8ee 2020). The focus is primarily on mitigating issues stemming from centralized discovery indexes (as opposed to knowledge bases) and on promoting transparency around the content and indexing level of metadata being ingested and displayed to users. In particular, it sets out the technical recommendations for metadata transfer between content providers and discovery vendors to ensure timely and consistent updates; recommendations on communicating to library stakeholders the content availability, metadata display rights, and degree of indexing for ingested metadata; standards for fair and unbiased linking; and how usage statistics should be gathered and reported to discovery service customers.

One of the most beneficial aspects of this recommended practice is the increased transparency for content coverage within discovery service indexes. Because the metadata supplied by content providers undergoes normalization and merging processes during ingestion, the records presented to end users in their search results often contain metadata elements from multiple providers. As explained in the recommended practice, "For a journal article . . . its full text might be contributed by the primary publisher, citation data from the providers of an aggregated database, and abstracts or controlled vocabulary terms may be provided by yet another provider" (Open Discovery Initiative Standing Committee 2020, 2). This mix-and-match approach, while at times beneficial for users, makes it difficult for libraries to evaluate the degree of exposure their acquired content has within the index. Gaps in coverage may exist within a collection a library assumes is fully and robustly covered. Further complicating this issue are the private agreements content providers have with the discovery vendor, which influence how, when, and to whom the metadata can be exposed (e.g., only to subscribing institutions or to everyone). If this recommended practice is widely adopted, libraries will have access to reports regarding the coverage and index of their collections and can take steps to mitigate issues around missing or hard-to-find items.

E-book Bibliographic Metadata Requirements in the Sale, Publication, Discovery, Delivery, and Preservation Supply Chain

The NISO Recommended Practice for E-ebook Bibliographic Metadata (NISO RP-29-2022) establishes best practices for naming, identifying, and describing e-books in order to ensure effective and consistent communication across stakeholder organizations (NISO E-book Bibliographic Metadata Requirements in the Sale, Publication, Discovery, Delivery, and Preservation Working Group 2022). The recommended practice identifies the minimum requirements for e-book metadata, including five essential elements (titles, names, dates, book identifiers, and subjects) as well as three version-specific metadata elements: format, constraints on use, and Uniform Resource Identifier (URI) or Internationalized Resource Indicator (IRI). If widely adopted, these best practices will allow libraries to more easily identify and manage their e-book holdings within various knowledge management systems.

Video and Audio Metadata Working Group

The NISO Video and Audio Metadata Working Group was formed in 2019 to evaluate what metadata elements are needed to sufficiently identify and describe online media content. The working group aims to create a new NISO recommended practice that will serve as a guideline for the creation and dissemination of metadata for administrative, semantic, technical, use rights, and accessibility information. If widely adopted, these recommended practices will improve the dissemination, discoverability, and indexability of video and audio content in both library and stakeholder systems. The working group will provide a draft of its recommended practices for public comment in 2022.

Unique Electronic Resource Package Identifiers Working Group

The Unique Electronic Resource Package Identifiers Working Group is a newly proposed NISO working group whose aim is to "evaluate and create recommendations for unique package identifiers that provide disambiguation across the supply chain" (NISO 2021). Currently, purchased or licensed e-resource packages are identified by name only. This leads to confusion among stakeholders, who may struggle to identify packages on past invoices, within licenses, or in a knowledge base, especially when those names have changed over time. By recommending best practices for unique identifiers for e-resource packages, the working group hopes to alleviate that confusion and improve the efficiency and accuracy of the work of all stakeholders. They also anticipate this work will support the adoption of KBART Automation. This working group is currently in the formation stages. The roster is scheduled to be announced in 2022.

Access and License Indicators (ALI)

The NISO Access and License Recommended Practice (RP-22-2015), approved on January 5, 2015, aims to address two pain points around e-resource access: identifying "free-to-read" content and providing information on what reuse rights might be available to the reader regarding that content (NISO Access and License Indicators Working Group 2021). The working group developed two metadata fields, expressed in XML as <free_to_read> and <license_ref>, that publishers and content providers could include alongside standard metadata describing a work. These fields could then be used on the publisher's platform or transmitted to downstream systems, such as aggregators, A&I services, and discovery layers, to display icons or verbiage indicating the work's access status to the end user.

While both metadata fields have the potential to mitigate access issues, the <free_to_read> field is likely to show a more immediate effect. The term "free-to-read" is used within the recommended practice to refer to any work "that is accessible to read online without charge or authentication (including registration) to any person with access to the internet" (NISO Access and License Indicators Working Group 2015, 1). The term was adopted instead of "open access," which can carry a variety of meanings and nuance. The free-to-read field fills an important gap in metadata—particularly for articles—by not only identifying freely accessible content but also, with the use of start and end date attributes, taking into account changes in access status "where content was free-to-read for a period of time or after a particular date," such as with embargoes or other delayed access models (NISO Access and License Indicators Working Group 2015, 5).

Before the introduction of this metadata field, access status was typically conveyed to the discovery layer from a link resolver knowledge base or an ERMS and, as a result, was managed at a journal or volume level rather than the article level. This would lead to confusion by end users when accessing hybrid journals, where some but not all articles are made freely available to readers. Widespread adoption of this metadata field for articles would help alleviate the frustration end users feel when encountering hybrid journals and other complex access models, where articles change their access status over time. In turn, this may result in less user error when reporting denials of access to library staff.

Authentication Services

Complicated library authentication systems historically have been a pain point for end users and librarians alike. Services have emerged in recent years aimed at alleviating the frustration. We highlight two here.

The IP Registry

The IP Registry is a service offered by PSI Ltd., a for-profit company based out of the UK. Libraries can register their IP address ranges with the service for free, and the service in turn disseminates the ranges via API to participating publishers and content providers. This service aims to save the time and effort of librarians by acting as a centralized location for them to check and update their institutional IP ranges. It also aims to benefit publishers by ensuring they receive timely, validated IPs through an automated process, thus preventing errors from manual IP entry.

SeamlessAccess

SeamlessAccess is a free service aimed at streamlining and securing the remote user authentication process. An outgrowth of the Resource Access for the 21st Century (RA21) initiative, SeamlessAccess promotes the use of federated identity management (FIM) instead of IP addresses to handle user authentication. For libraries and academic institutions that use a FIM authentication tool, such as InCommon (Shibboleth) or OpenAthens, it provides a consistent log-in experience for users on participating content and discovery platforms. This includes equipping platforms with a uniform WAYF (Where Are You From) searchable menu, standardized institution metadata, and a persistence service so users do not need to reauthenticate when visiting another SeamlessAccess-enabled platform.

SeamlessAccess has the potential to reduce access issues related to IP authentication and further streamline the FIM log-in experience. If widely adopted by libraries and content platforms, it may lessen user error around the authentication process, which currently relies on end users utilizing different software and navigational starting points, such as VPNs or proxied URLs, depending on their physical location. It also has the potential to reduce the impact of security breaches on content providers and libraries because FIM authentication is inherently more secure than IP authentication.

Other Initiatives

Transfer Code of Practice

The NISO Transfer Code of Practice (RP-24-2019) is a set of best practices for when an electronic journal is transferred from one publisher to another (NISO Transfer Standing Committee 2019). Originally developed as a UKSG initiative in 2006, Transfer was later adopted by NISO as a recommended practice in 2014 and updated to its current version in 2019. Transfer helps to ensure continuous access of electronic journals during the publisher transfer process by establishing what information at minimum needs to be communicated to various stakeholders, including customers, readers, content recipients, and transfer partners, and within what time frame. The Transfer Alerting Service (TAS) was developed to support this communication. Through TAS, libraries can sign up for e-mail alerts of upcoming journal transfers, as well as search a database of previous transfers.

> Librarians are encouraged to try the enhanced transfer alerting service and contact any librarians on the standing committee if they have questions. If there are any publishers that are not currently Transfer-compliant, please let a standing committee member know so that the publisher can be contacted about becoming compliant. (Copeland 2019, 160)

TAS is currently hosted by the ISSN International Centre.

Content Platform Migrations

The NISO Content Platform Migrations Recommended Practice (RP-38-2021) aims to mitigate access disruptions that occur when publishers change content-hosting platforms by outlining actions stakeholders should take when performing the migration (NISO Content Platform Migrations Working Group 2021). The recommended practice covers items related to linking (redirects, link resolvers, authentication), content migration, metadata migration (KBART, MARC, ISSN/ISBN), user and administration accounts, usage statistics, and stakeholder communication.

References

Copeland, Jessie. 2019. "The Transfer Code of Practice: Overview and Updates." *Serials Librarian*, 76, no. 1–4: 159–61. https://doi.org/10.1080/0361526X.2019.1540267.

Derouchie, Elizabeth Levkoff, Beth Ashmore, and Eric Van Gorden. 2021. "Knowledge Bases: The Heart of Resource Management." *Serials Librarian* 80, no. 1–4: 117–21. https://doi.org/10.1080/0361526X.2021.1884488.

KBART Automation Working Group. 2019. *KBART Automation: Automated Retrieval of Customer Electronic Holdings*. NISO Recommended Practice, NISO RP-26-2019, June 18. Baltimore, MD: National Information Standards Organization (NISO). https://groups.niso.org/higherlogic/ws/public/download/21896.

KBART Phase II Working Group. 2014. *Knowledge Bases and Related Tools (KBART) Recommended Practice*. NISO Recommended Practice, NISO RP-9-2014. Baltimore, MD: National Information Standards Organization (NISO). https://groups.niso.org/higherlogic/ws/public/download/16900.

NISO (National Information Standards Organization). n.d. "KBART Phase I." https://www.niso.org/node/15671.

———. 2021. "New NISO Project—Package Identifiers." News release, September 14. https://www.niso.org/press-releases/2021/09/new-niso-project-package-identifiers#:~:text=The%20NISO%20Unique%20Electronic%20Resource,used%20across%20the%20supply%20chain.

NISO Access and License Indicators Working Group. 2015. *Access License and Indicators*. NISO Recommended Practice, NISO RP-22-2015, January 5. Baltimore, MD: National Information Standards Organization (NISO). https://groups.niso.org/higherlogic/ws/public/download/14226/rp-22-2015_ALI.pdf.

———. 2021. *Access and License Indicators*. NISO Recommended Practice, NISO RP-22-2021. Baltimore, MD: National Information Standards Organization (NISO). https://groups.niso.org/higherlogic/ws/public/download/26339/RP-22-2021_ALI.pdf.

NISO Content Platform Migrations Working Group. 2021. *Content Platform Migrations*. NISO Recommended Practice, NISO RP-38-2021, November 18. Baltimore, MD: National Information Standards Organization (NISO). https://groups.niso.org/higherlogic/ws/public/download/26321.

NISO E-book Bibliographic Metadata Requirements in the Sale, Publication, Discovery, Delivery, and Preservation Working Group. 2022. *E-Book Bibliographic Metadata Requirements in the Sale, Publication, Discovery, Delivery, and Preservation Supply Chain*. NISO Recommended Practice, NISO RP-29-2022, January 29. Baltimore, MD: National Information Standards Organization (NISO). https://groups.niso.org/higherlogic/ws/public/download/26477.

NISO Transfer Standing Committee. 2019. *Transfer Code of Practice*. NISO Recommended Practice, NISO RP-24-2019. Baltimore, MD: National Information Standards Organization (NISO). https://groups.niso.org/higherlogic/ws/public/download/21330/Transfer_NISO_RP-24-2019.pdf.

Open Discovery Initiative Standing Committee. 2020. *Open Discovery Initiative: Promoting Transparency in Discovery*. NISO Recommended Practice, NISO RP-19-2020, June 22. Baltimore, MD: National Information Standards Organization (NISO). https://groups.niso.org/higherlogic/ws/public/download/24113/NISO_RP-19-2020_ODI_Open_Discovery_Initiative.pdf.

New Developments in Library Discovery and Access

The library and scholarly publishing ecosystem is ever evolving. It can be difficult to capture a snapshot of this evolution without risking irrelevancy or obsolescence. Libraries are deeply affected by any advancements occurring within the information technology, information security, scholarly publishing, and library discovery service industries. Throughout this chapter we touch upon a broad range of technological developments, the new opportunities for access failure that they will elicit, and how these developments will influence library troubleshooting efforts.

New Developments in Linking: LibKey API and GetFTR

Struggles with the chronic OpenURL link resolver issues have given rise to new linking applications aimed at providing one-click access to full-text article content. Third Iron's LibKey API and its suite of products, including a discovery integration (LibKey Discovery), a browser extension (LibKey Nomad), a DOI and PMID article finder (LibKey.io), and a link resolver accelerator (LibKey Link), have become a well-established service in academic libraries. Through LibKey, rather than selecting links from a long list in the resolver menu, users are presented with links directly to article PDFs based on the library's electronic holdings. It also connects users to open-access resources that may not be discoverable from other library tools. LibKey Discovery puts this functionality within the library's discovery service, but other applications of LibKey, such as LibKey Link, enable one-click access within other interfaces, such as A&I databases, aggregators, and Google Scholar.

Get Full Text Research (GetFTR) is another one-click-access application new to the scholarly publishing market. Unlike LibKey, which relies upon the subscribing library's knowledge base holdings and its own knowledge base of open-access content to deliver access, GetFTR uses its API to check an institution's entitlements on participating publishers' platforms. Since GetFTR is a service marketed to publishers for inclusion on their platforms, there is no financial investment on the library's end. And, as GetFTR says on its website, "Libraries and researchers do not need to opt-in, register, or download any new software" (GetFTR, n.d.). The one-click links will simply appear on participating publisher sites.

GetFTR is limited in several capacities, however, as compared to LibKey. The first is authentication. While LibKey is able to integrate with the full range of library authentication methods (IP, proxy, VPN, FIM), GetFTR was created primarily to function alongside SeamlessAccess, a FIM initiative. It has since added IP authentication methods, but this is a recent development, and it is unclear yet how well (or confusing) the integration is. Next, LibKey is able to be implemented across a variety of search interfaces, including major players such as Google Scholar and PubMed, but GetFTR is currently limited to subscribing publisher platforms. Aggregators and A&I databases have yet to sign on. This, too, may change in the future—GetFTR is currently seeking aggregators to test its product and Elsevier has launched a new discovery-esque pilot featuring GetFTR—but currently the one-click access is of limited use. Finally, assuming GetFTR is integrated with aggregators, questions remain about fair linking practices and how usage statistics will be counted. Because LibKey is a library service, libraries have more ability to configure linking options, such as choosing whether or not to link to prepublication manuscript (i.e., non–Version of Record). Libraries are also able to add their link resolver menu as a fallback option should no full-text holdings be found. GetFTR, conversely, is a publisher service relying on publisher entitlements. Therefore, linking configurations must be agreed upon by the participating publishers and integrators, including whether or not an article hosted on the publisher site will receive linking priority over the same article hosted on an aggregator site. However, if GetFTR is able to work through its current limitations and answer these questions, it may become another well-established linking option on which researchers and libraries alike can rely.

New Horizons for Discovery: Elsevier, Yewno, and EBSCO Concept Maps

ScienceDirect Pilot

In early 2022, Elsevier launched a pilot project intended to alleviate the frustration end users experience when conducting literature reviews. Elsevier has partnered with publishers, including the American Chemical Society, the Royal Society of Chemistry, Taylor & Francis, and Wiley, for a six-month project to understand how it can help researchers find and access content more easily. During the pilot, researchers will be able to search and browse more than 70,000 articles in thirty-five journals in two major disciplines from participating publishers alongside Elsevier's content on ScienceDirect (L'Huillier 2022). Researchers will have an integrated search, browse, and display experience on ScienceDirect; however, content access and delivery will remain distributed across the multiple publisher platforms (Hinchliffe 2022).

Elsevier has been an innovator in the search and linking sphere since the early nineties. In the early 2000s, for example, it was experimenting with a linking program called ScienceDirect Gateway, which allowed linking between the ScienceDirect platform and affiliated publisher websites. It is no surprise, therefore, that Elsevier was an initial sponsor of GetFTR and is using it in its current pilot project to connect users to the full text on the participating publisher platforms. GetFTR in combination with SeamlessAccess aims to streamline navigation for users, whether they are starting their research from their library's website or the web at large, and whether on or off site. It will also reduce frustration by having scholarly content for a single discipline robustly represented on a single search interface, which will certainly increase discovery and end user satisfaction.

Elsevier may have launched this pilot program in response to websites like Sci-Hub and ResearchGate, which have been hubs for illegal sharing of academic papers. While some publishers, such as Springer Nature and Wiley, have syndicated their content to ResearchGate so users are directed to the article's validated version of record, Elsevier has taken a different tack with these websites and initiated lawsuits. If Elsevier is successful in its pilot and expands to include other disciplines, this may signal the start of other content providers developing similar services for their own disciplines.

Elsevier's pilot may have implications for librarians tasked with ensuring their users can access subscribed resources. If issues with GetFTR linking arise, librarians may find themselves stuck in the middle, trying to troubleshoot and resolve the issue between the service and the content providers. Ideally, though, the linking will be more reliable than OpenURL and individual librarian oversight will be reduced as a result.

Visual Concept Mapping

Visual concept maps, or knowledge graphs, are another innovation in search and discovery to pick up steam in recent years. Concept maps, like those offered from Yewno and EBSCO, enhance discovery searches by showcasing relationships between terms in the form of a visual, web-like graph. Unlike traditional discovery, which relies upon controlled vocabulary, subject headings, and keyword indexing, concept maps analyze the text of documents through machine-learning (AI) programs to extract contextual relationships between assorted topics. Because these programs learn as they ingest new material and as users interact with them, new relationship threads can strengthen or lessen with time, leading to users unearthing new, at times unexpected, documents and research concepts. Concept maps have the potential to overcome the gap between controlled vocabularies, with which end users are often unfamiliar, and natural language.

The potential implications for troubleshooting are interesting to consider. Librarians are accustomed to reporting discovery service issues such as broken links and incorrect metadata source records for e-books, e-journals, streaming video, and so on. Concept maps may introduce new opportunities for failure in the form of incorrect subject assignments, content display issues, inaccurate subject associations, or other creative malfunctions.

Automation of E-resource Workflows

Libraries are increasingly looking for ways to automate their e-resource management workflows. KBART Automation, which we discussed in the last chapter, is now being employed by several vendors to automatically set e-resource holdings for libraries using Alma/Primo. EBSCO, too, has been implementing automated workflows between its various services. EBSCO Subscription Services (ESS) Auto-Population in Holdings Management offers a way to automate the knowledge base holdings selection process. However, unlike KBART, this service can be activated only by libraries that employ both ESS (EBSCOnet) and EBSCO Discovery Services. As described on EBSCO's support center, this service "automates an otherwise manual library workflow to update your holdings to reflect your EBSCO E-journal and Package Subscription orders through ESS" (EBSCO Connect 2021). With ESS Auto-Population, new orders are processed and holdings are mapped to resources in EBSCO's Global Knowledge Base daily.

Regardless of the best intentions, many of the stark realities of acquisitions and cataloging will still necessitate a review of a library's holdings despite having ESS Auto-Population or KBART Automation enabled. For acquisitions, review may still be needed due to consortial purchases that experience annual updates with additions and cancellations to individually tracked titles. For cataloging, e-journal title changes and publisher transfers are likely to continue to wreak their current level of havoc regardless of attempts at automation.

Automated holdings attempts can also make traditional holdings tracking workflows more opaque. For example, ESS Auto-Population can set only library holdings that were ordered through ESS. Libraries currently cannot import comprehensive holdings coverage, which would include both current orders and previous orders with perpetual access acquired through other subscription agents, into EBSCOnet in order to be included in a library's holdings. EBSCO does provide options to prevent overwriting custom holdings changes, thereby preserving the manual efforts necessary to record custom access for a library's holdings.

There are still many benefits to automated holdings management, such as reduced staff time, fewer entitlements lost in translation from invoice to knowledge base holdings, and quicker access to content. Another significant advantage of KBART Automation is the ability to push out substantial updates at a moment's notice. During the COVID-19 pandemic, many content providers allowed time-limited free offers to their content, and these updates were able to be rapidly disseminated to libraries that had established KBART Automation.

Content providers, subscription agents, and knowledge base vendors will likely continue to form additional innovative partnerships to improve customer satisfaction through the rapid dissemination of holdings. These new efforts at automation are more likely to succeed in reducing access disruptions if they adhere to the various metadata standards that were covered in the last chapter and if vendors continue to closely partner with libraries to better learn the daily necessities required for adequate holdings management.

Moving to the Cloud

One of the most significant moves libraries have made in recent history is the shift from locally hosted library systems to library services platforms, such as FOLIO, WorldShare Management Services, and Alma, which are hosted in the cloud. Library services are not the only industry moving their systems into the cloud. Adoption of cloud infrastructure and platform services, such as Amazon Web Services (AWS), Microsoft Azure, and Google's cloud services, has become increasingly popular in recent history. However, the downside of this widespread adoption is that service outages could affect a library's entire access chain: from LSP to discovery service to vendor platform. Extensive service outages, such as the ones experienced by AWS in 2017 and 2021, are hugely disruptive for library users and well beyond the power of libraries to fix. However, for better or worse, they are much more clear-cut for librarians to troubleshoot.

The Death of IP Authentication

Cloud Application Security and Ransomware Protection Software

As institutions increasingly move their software applications to the cloud, new concerns emerge around cyber security. Many institutions are investing in cutting-edge cloud application security (CAS) and ransomware protection software to help protect their users, but such software can have unintended consequences for libraries, including disrupting IP authentication. Although libraries have employed IP authentication as the gold standard for many years, "most other consumer or industry vendor access methods stopped using IP authentication long ago" (SeamlessAccess.org, n.d.). As a result, many IT professionals are unaware of how these applications can affect library e-resource access.

At the 2022 Electronic Resources and Libraries Conference, one library shared its experience with cloud application security being installed on institutional laptops. On-site users at the institution and off-site users utilizing the VPN encountered paywalls when trying to access library e-resources. When the librarians investigated, they discovered the users' IP addresses were outside their institutional ranges. After contacting their institution's IT department, they discovered that the recently deployed CAS software was responsible for users being reassigned an IP address outside of normal institutional ranges. This in turn meant that the users could not access any library e-resources with an IP address outside institutional ranges that their content providers did not recognize. While the library at the conference said that it had no permanent solutions, its IT department was working with its CAS vendor to implement the necessary exceptions.

Another cyber security solution able to wreak havoc on library e-resource access is ransomware protection software. Enterprise ransomware protection software solutions behave and function in different ways (some of which are proprietary trade secrets) in response to the different types of malware that could infect an institution's computers. Sometimes this behavior can adversely affect e-resource access. For example, ransomware protection software may block an institution's on-site traffic from accessing IP addresses previously flagged for having unusually high traffic or for containing suspicious adware. If a content provider's IP erroneously gets flagged, this could mean on-site users are blocked from accessing that platform. The interim solution would be to make necessary exceptions for IP addresses originating from e-resource content providers.

Browser Vendors Work to Increase User Privacy

Driven by online privacy fears, browser vendors are reconsidering long-held practices of how they track and target advertising to their users. In response to events like the 2018 Cambridge Analytica scandal and European regulators enacting the General Data Protection Regulations, browser vendors have been developing new security measures that will in turn greatly increase user privacy. Unfortunately for libraries, an unintended consequence of these proposed changes is that they may put an end to IP authentication as we know it. In an effort to preserve privacy, some browser vendors are introducing technology to obfuscate user IP addresses, which would prevent those utilizing these browsers from accessing IP authenticated e-resources. FIM authentication, including initiatives like SeamlessAccess, will also be affected. The browser technology changes being undertaken affect the way that cookies are stored. As SeamlessAccess.org explains, "The browser cannot tell the difference between a cookie that lets a service know the user is authenticated from a cookie that allows an advertiser network to track a user around the web" (SeamlessAccess.org, n.d.). Currently, users can adjust their privacy settings on browsers employing this technology in order to allow platforms to read their IP address or cookies. However, such privacy measures are increasingly the default in browser settings.

This has tremendous implications for troubleshooting. Time-tested troubleshooting techniques, like recommending that off-site users employ the institution's VPN, may no longer be valid in an environment where institutional machine IP addresses cannot be used to authenticate access. Moving away from IP authentication would require a great amount of adjustment for libraries, and end users would be negatively affected while the new methods of authentication are worked out. Such a paradigm shift would no doubt cause ripple effects for years to come as libraries reorient themselves to new means of authentication and new troubleshooting best practices to deal with the issues that would inevitably spring up.

References

EBSCO Connect. 2021. "ESS Auto-Population in Holdings Management—Frequently Asked Questions." July 8. https://connect.ebsco.com/s/article/ESS-Auto-Population-in-Holdings-Management-Frequently-Asked-Questions?language=en_US.

GetFTR. n.d. "Why GetFTR and FAQs." https://www.getfulltextresearch.com/why-use-getftr/.

Hinchliffe, Lisa Janicke. 2022. "Elsevier's ScienceDirect as Content Supercontinent?" *Scholarly Kitchen* (blog), January 18. https://scholarlykitchen.sspnet.org/2022/01/18/sciencedirect-as-content-supercontinent/#comments.

L'Huillier, Rose. 2022. "ScienceDirect Pilot Aims to Improve Research Discovery and Access." Elsevier, January 18. https://www.elsevier.com/connect/sciencedirect-pilot-aims-to-improve-research-discovery-and-access.

SeamlessAccess.org. n.d. "LEARNING-CENTER > FAQ on Browser Privacy Changes and Library Resource Access (Or Why Your IP Authentication Is About to Break)." https://seamlessaccess.org/learning-center/browser-faq/#question-1-what-is-this-accessing-remote-content-issue.

Conclusion

The current landscape of electronic resources access issues is ever-evolving and greatly influenced by advances in information technology. In this report, we have defined the technological components required to facilitate e-resource access and discussed how the limitations of these components directly correlate to the amount of electronic resource troubleshooting required to keep them running smoothly. We have attempted to include and define all points of access common to library access chains; however, any attempt at comprehensiveness will invariably omit relevant systems, tools, or metadata.

Once a troubleshooter is able to understand their library's access chain, they are better equipped to diagnose and resolve access disruptions. We have gone into great detail concerning the common methods of authentication, systems, and tools used by libraries, which should inform a troubleshooter's base knowledge. With this base knowledge, a troubleshooter can then consider the source and types of metadata that flow in and out of their library's access chain. With this understanding they are ready to identify the common points of failure inherent to their systems and to begin to diagnose their access disruptions. Tools and techniques for diagnosing are many and varied, but we hope the sampling we have provided will prove useful and offer inspiration for discovering local solutions. Finally, there are many ongoing efforts that attempt to mitigate access disruptions. The contributions of the various NISO standing committees and working groups to the health of the discovery environment cannot be overstated.

New developments in information technology and the library discovery market will greatly impact troubleshooting efforts in the years to come. Much like the cataclysmic event that moving from AACR2 to RDA represented for cataloging librarians, troubleshooting librarians will be dealing with the fallout from the phasing out of IP authentication for the foreseeable future. As holdings management shifts away from libraries and toward vendors, only time will tell how well these new automated workflows will be implemented. Logic states that troubleshooters will spend less time dealing with broken link issues and more with errant metadata and entitlement inaccuracies. Individual librarian oversight will likely be reduced as a benefit of these new technological efforts. However, much of the work of caring for these systems will not disappear but instead be transformed into new workflows troubleshooters are not yet familiar with.

Despite the great advances in improving the discovery, access, and management of e-resources, it may be premature to declare victory over any particular area of troubleshooting just yet. As long as there are electronic resources, there will be a need for a librarian to usher them through their life cycle. Troubleshooting librarians are irreplaceable.

Statement of Ownership, Management, and Circulation

Library Technology Reports, Publication No. 024-897, is published eight times a year by the American Library Association, 225 N Michigan Ave, Suite 1300, Chicago (Cook), Illinois 60601-7616. The editor is Samantha Kundert, American Library Association, 225 N Michigan Ave, Suite 1300, Chicago, IL 60601-7616. Annual subscription price, $340.00. Printed in U.S.A. with periodicals class postage paid at Chicago, Illinois, and at additional mailing offices. As a nonprofit organization authorized to mail at special rates (DMM Section 424.12 only), the purpose, function, and nonprofit status of this organization and the exempt status for federal income tax purposes have not changed during the preceding twelve months.

(Average figures denote the average number of copies printed each issue during the preceding twelve months; actual figures denote actual number of copies of single issue published neared to filing date: July 2022 issue.) Total number of copies printed: average, 286; actual, 254. Paid distribution outside the mails including sales through dealers and carriers, street vendors, counter sales, and other paid distribution outside the USPS: average 51; actual, 25. Total paid distribution: average, 212, actual, 159. Free or nominal rate copies mailed at other classes through the USPS (e.g., First-Class mail): average, 0; actual, 0. Free or nominal rate distribution outside the mail (carriers or other means): average, 6; actual, 5. Total free or nominal rate distribution: average, 6; actual, 5. Office use, leftover, unaccounted, spoiled after printing: average, 68; actual, 90. Total: average, 286; actual, 254. Percentage paid: average, 97.42%; actual, 96.95%.

Statement of Ownership, Management and Circulation (PS Form 3526, July 2014) filed with the United States Post Office Postmaster in Chicago, August 2, 2022.

Library Technology
R E P O R T S

Upcoming Issue	
Nov/Dec 58:8	**Bibliometrics Tools and Technologies in Academia** by Laura Bredahl

Purchase single copies in the ALA Store
alastore.ala.org

A Note to Our Subscribers

As a subscription-based publication, ***Library Technology Reports*** will sunset with the December 2022 issue. After that time, it will be available for single-issue sales only. Subsequently, no new ***Library Technology Reports*** subscriptions or renewals will be accepted. If you have questions about your subscription, please contact us at subscriptions@ala.org or call toll free at (800) 545-2433, ext. 4299.