

Change Auditing and Recovery for optimizing the use of Active Directory in the NRW Fiscal Authority



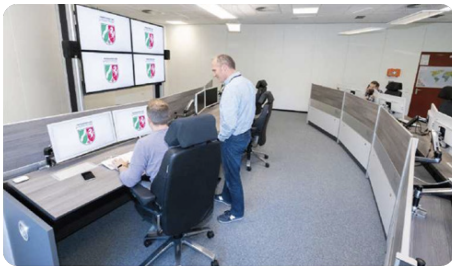
The North-Rhine Westphalian fiscal authority comprises the Finance Ministry of the State of North-Rhine Westphalia as the highest state institution along with various higher regional authorities and mid-level authorities such as the State Office of Salaries and Pensions, the State Finance Office, the Regional Finance Authority, as well as the individual tax offices including company audits and tax fraud investigations as lower-level state institutions.



Even after the start of productive operation, we have always had somebody with a great deal of expertise at our side. But operation is so problem-free that we only rarely have to draw on that resource.

Dietmar Rilke, Head of Windows Systems at the NRW Fiscal Authority

The fiscal authority also runs training institutions such as the University of Finance at Schloss Nordkirchen, the Regional School of Finance, and its academy of professional development. The fiscal authority's central data center also functions as top-level regional processing institution responsible for the operation of the entire IT infrastructure. This data center serves as the central service provider for approximately 140 locations with ca. 30,000 users across the state. Naturally, information technology is a sensitive subject for any fiscal authority, since it processes largely confidential and personal data. This makes it essential to set up and then implement highly detailed rules about which personnel members have access to which types of data and applications. The Fiscal Authority of the State of North-Rhine Westphalia uses Microsoft's Active Directory (AD) to securely manage its users and their access rights and permissions. AD serves as central directory, managing all IT objects such as users, groups, applications, and devices. It also allows administrators to control access to resources determining and managing user permissions.



Active Directory uses auditing

As a central service, AD has a great deal of significance when it comes to the availability of data and applications across North-Rhine Westphalia's entire network of financial institutions. Failures, even partial ones, invariably lead to personnel being unable to complete their tasks, limiting the functionality of all departments across the board. Furthermore, AD offers no simple, in-application means of recovery, so that such problems can be solved only manually and with high personnel and man-hour costs. In particular AD's protocol functions are extremely limited, often making it impossible to track changes. At the same time, it is usually those very changes that lead to errors and failures. Just such a partial failure of Active Directory was the Fiscal Authority's main reason to look for a solution that would enable efficient change management as well as comprehensive auditing. In addition, the solution had to offer a simple way to fully recover objects in AD after potential failures, and to roll back changes, ideally in increments. Auditing would also support revision-proof

electronic filing, and would enhance security, since nowadays the early phase of most cyber-attacks focuses on changes to the Active Directory system in order to give attackers additional room for exploits using expanded access rights. It was a recommendation that first attracted the attention of Dietmar Rilk, head of the Authority's Windows Systems division, and his team to Cygna Labs and its Cygna Auditor platform, distributed in Germany by N3K Network Systems, among others. The application's function module "Cygna Auditor for Active Directory" monitors all administrative activity within the critical directory service Active Directory in real time, thus giving administrators the ability to recognize all changes and, if desired, raise alarms on unauthorized changes in real time. Based on these audit data, any changes can be reversed if necessary—regardless of whether they were caused by faulty configuration or external attack. For this purpose, the Cygna Auditor platform and its "Cygna Recovery" function module offers an accurate rollback function based on the collected AD audit data with no back-up time point. This means that data can be restored for any desired point in time, with a high degree of granularity of all AD objects down to the attribute level, even incrementally, if called for.



“In planning and implementation phases, working with N3K as system integrator was extremely easy and unobtrusive.”

Dietmar Rilk, Head of Windows Systems at the NRW Fiscal Authority

Centralized Event Monitoring and Evaluation

Since the previous partial failure had been classified as a serious security risk, the Fiscal Authority was able to implement the Cygna Auditor platform in August 2021 in compliance with public procurement law. "What was particularly important to us was being able to centrally

monitor and evaluate events in AD," Dietmar Rilk explains. "That is the precondition for recognizing critical events and being able to offer a largely automated reaction to them rather than just spitting out alarms on the console." What is more, its seamless documentation of access and changes meant that the Cygna Auditor platform and its "Cygna Auditor for AD" simplified the compliance with the GDPR and all specifications of Germany's BSI (Bundesamt für Sicherheit in der Informationstechnik, Federal Office for Information Security). In particular, traceability of all changes in AD was one of the main reasons for choosing the Cygna Auditor platform. Although Active Directory, too, offers native event logging on the domain controller, old log entries are overwritten with newer entries every 30 to 60 minutes depending on the configuration, so that there is no long-term documentation. The Cygna Auditor platform, on the other hand, uses an independent SQL database for storing events, thus offering not only a capacity limited only by the storage medium, but also immense ease of access. All Active Directory changes are tracked seamlessly using an independent mechanism without recourse to the native log files. This ensures better data quality with approximately 75% lower data volume. In addition, the Cygna Auditor platform boasts a simple, modern, and clear-cut web GUI allowing simple, cross-platform operability. At the Fiscal Authority of the State of North-Rhine Westphalia, the Cygna Auditor platform and its function module "Cygna Auditor for AD" and "Cygna Recovery for AD" support an environment in which the management of hardware, software, and identities is highly centralized. "Yes, there are responsibilities delegated to our individual locations, but there are no local administrators," Rilk says. "All administration is handled centrally at our data center, and higher-level access rights at the locations are granted only if there are compelling reasons to do so—and even then, only temporarily. We consistently implement the principle of least privilege." The Fiscal Authority, Rilk adds, simplifies centralized administration through a high degree of standardization and harmonization, with all servers and clients sharing identical configurations.

“Since roll-out in August of 2021, the Cygna Auditor platform and its function modules 'Cygna Auditor for AD' and 'Cygna Recovery for AD' have been in failure-free operation at the Fiscal Authority.”

Dietmar Rilk, Head of Windows Systems at the NRW Fiscal Authority

For more information about Cygna Labs products and services, please contact us at

Toll Free: **(844) 442-9462** | International: **+1 (305) 501-2430** | Email: sales@cygnalabs.com

Cygna Labs Corp. | 1688 Meridian Ave, Suite 1010 | Miami Beach, FL 33139 | United States