nevisReports – Governance Reporting

Teaser

Governance Reporting allows the analysis of normal and abnormal behavior of your security infrastructure. It provides detailed, near real-time reports across all main NEVIS components. Governance reports are highly customizable to serve many different audiences from IT professionals to risk managers.

Benefits

nevisReports aggregates log data and information from various sources into easy-to-use reports for an **improved insight into system activity**. It has a scalable architecture that allows processing large amounts of data as well as fast searches.

nevisReports provides detailed, near real-time governance reports on the usage of all main components of your NEVIS Security Suite. In conjunction with the governance dashboard, you will be able to thoroughly **analyze normal and abnormal behavior**, which is crucial in **minimizing potential threats**.

Additionally, the governance reports are highly customizable in order for you to generate the reports most relevant to you. They can be tailored to the requirements of any organization that wants to analyze the usage patterns of its NEVIS environment.

What is it about?

Security today requires a holistic view on granted authorizations, authentication processes and identities. Every day, you need to protect your business applications, manage on- and offboarding processes and perform other crucial security-related functions.

Without a tool to record all these events, managing the complexity of your system can be daunting.

nevisReports solves this problem. Its governance reports provide selected information on important events across the main components of your NEVIS Security Suite.

You will not need to manually interpret reports from different components – nevisReports gives you a unified view on your data.

Standard reports include session history, application usage and performance , roles and authorizations, and more.

Additionally, the governance reports are very flexible and offer a wide range of customization options. Various query filters allow the end users to configure the range of datasets to be included in the reports. This facilitates the creation of billing reports, audit reports, web usage time reports and many others.

Main features

- Topics available with standard reports:
  - Application usage and performance
  - Session history
  - Roles and authorizations granted
- Wide range of report customization options:
  - Billing reports
  - Audit reports
  - Web usage time reports
  - Access exception statistic reports
  - Reports on dormant accounts
- Data filtering and sorting
- Specification of report generation intervals, e.g., daily, weekly or monthly
- Support of PDF, Excel, HTML and other common output formats
- Report distribution through various channels such as e-mail, file sharing or the intuitive web GUI
- Report visibility can be restricted to specific user groups
- Reports always based on the latest data (near real-time reporting)

Switzerland ▪ AdNovum Informatik AG ▪ Roentgenstrasse 22 ▪ 8005 Zurich ▪ Switzerland ▪ +41 44 272 6111 ▪ info@nevis-security.ch ▪ www.nevis-security.ch
Singapore ▪ AdNovum Singapore Pte. Ltd. ▪ 3 Shenton Way ▪ #23-03 Shenton House ▪ Singapore 068805 ▪ +65 6536 0668 ▪ info@adnovum.sg ▪ www.nevis-security.sg
Germany ▪ NEVIS Office Germany ▪ Hubenstein 11 ▪ 84416 Taufkirchen ▪ Germany ▪ +49 8084 41 33 10 ▪ info@nevis-security.de ▪ www.nevis-security.de

Use Cases

Use case 1: Application usage and performance

You are the CTO of a company whose applications are protected by NEVIS. Every month, you want to inform your business managers of the trends in the usage of your applications.

Select the standard Traffic Statistics report. Then, set the report generation interval to monthly and specify the distribution channel, e.g., e-mail.

Your business managers now get a monthly e-mail presenting your applications' figures. They do not need to log in to nevisReports, and you do not have to remember sending a report every month.

Use case 2: Usage-based billing

The CFO of your company wants to invoice each department based on their usage of your applications. A custom report based on the standard Session History report, which shows the number of logins per month, can be developed. Define the cost per login, add it to the standard report and benefit from your custom billing report.

Use Case 3: Dormant accounts and authorizations

For a risk and compliance officer, it is important to know if issued accounts and authorizations are still necessary. It aids in evaluating your company's current exposure to threats and in making plans on how to minimize it.

The Dormant Accounts report lists enabled accounts that have been inactive for a specific, customizable time period. You can then decide what to do with these accounts, e.g., disable them to minimize your company's attack surface.

Unused authorizations per protected business application and per user can be withdrawn in the same way, based on information from the Dormant Authorizations report.

These reports combine data from the access as well as the identity layer.

Architecture – how does it work?

Figure 1 gives an architecture overview of nevisReports' detailed reporting feature.

nevisReports monitors and collects statistical data from nevisProxy, nevisAuth, and nevisIDM. However, it has only minimal influence on their operation.

With the collected data, nevisReports generates reports available via e-mail and the web. Users can choose between PDF, Excel and HTML format.

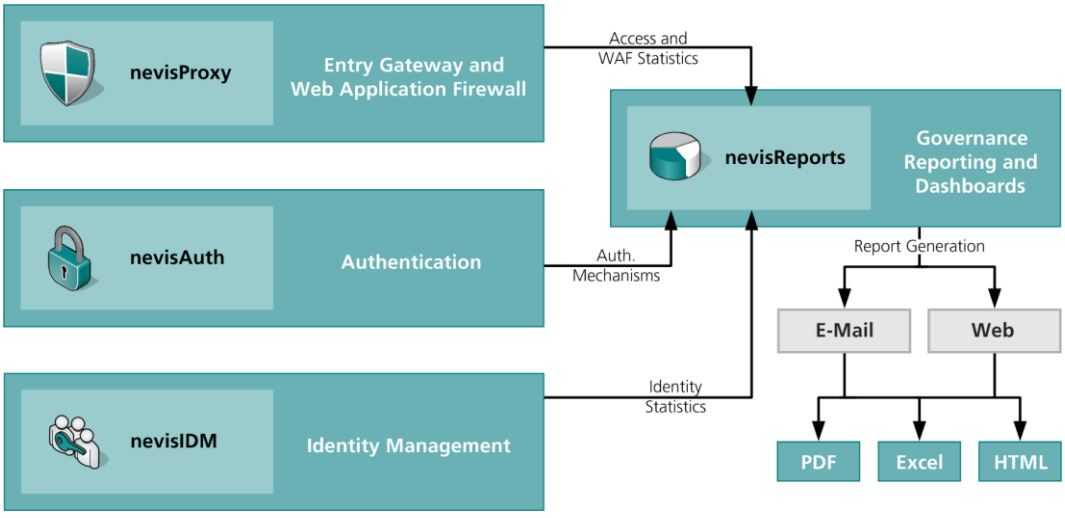

Figure 1 Architecture overview

Switzerland ▪ AdNovum Informatik AG ▪ Roentgenstrasse 22 ▪ 8005 Zurich ▪ Switzerland ▪ +41 44 272 6111 ▪ info@nevis-security.ch ▪ www.nevis-security.ch
Singapore ▪ AdNovum Singapore Pte. Ltd. ▪ 3 Shenton Way ▪ #23-03 Shenton House ▪ Singapore 068805 ▪ +65 6536 0668 ▪ info@adnovum.sg ▪ www.nevis-security.sg
Germany ▪ NEVIS Office Germany ▪ Hubenstein 11 ▪ 84416 Taufkirchen ▪ Germany ▪ +49 8084 41 33 10 ▪ info@nevis-security.de ▪ www.nevis-security.de