

Asitis Cloudware

Technical Information

Date

2019-03-12

asitis

Content

Content	1
1 Asitis Cloudware.....	2
2 Overall architecture.....	4
2.1 Scaling	5
2.2 Backup.....	6
3 Development, testing and testing tools	6
1. Development environment.....	6
2. Internal test environment.....	6
3. Acceptance test.....	7
4 API-information – Azure API Management.....	7
5 Security and Surveillance.....	8
5.1 Role based access system	9
5.2 Elastic Databases	10
5.3 Continuous development and continuous integration	11
5.4 Azure monitoring tools	12
5.5 Azure Application insights	12
5.6 Azure and network access.....	13
5.7 Compliance - Audit-logging of sensitive data.....	13
5.8 Hybrid solutions.....	13

1 Asitis Cloudware

Asitis Cloudware is a cloud-based ecosystem of financial services, developed to be at your service at anytime, anywhere, and on any device. The user interface is responsive which makes Cloudware available in any modern browser, pad, or smart phone depending on your preferences. Fast development cycles and agile launch solutions enable updating and deployment of services faster than ever before, without any longer interruptions.

The user experience is essential in Cloudware. Sophisticated interfaces and active feedback enable easy follow-up on ongoing Cloudware activities and how your business is developing. Intuitive dashboards and analyze-views provide you and your clients with real-time data at any time.

Built for the digital on-line community

Our driving force while developing Cloudware has been creating a scalable, mobile and secure real-time solution that meets the everchanging market needs. Time-to-market, security and integrability comes first.

Shorter lead times

In Cloudware, the time span from idea to live performance has been minimized through agile, cloud-based development and distribution.

Other benefits of an agile process are continuous deployment of adjustments as well as of new services.

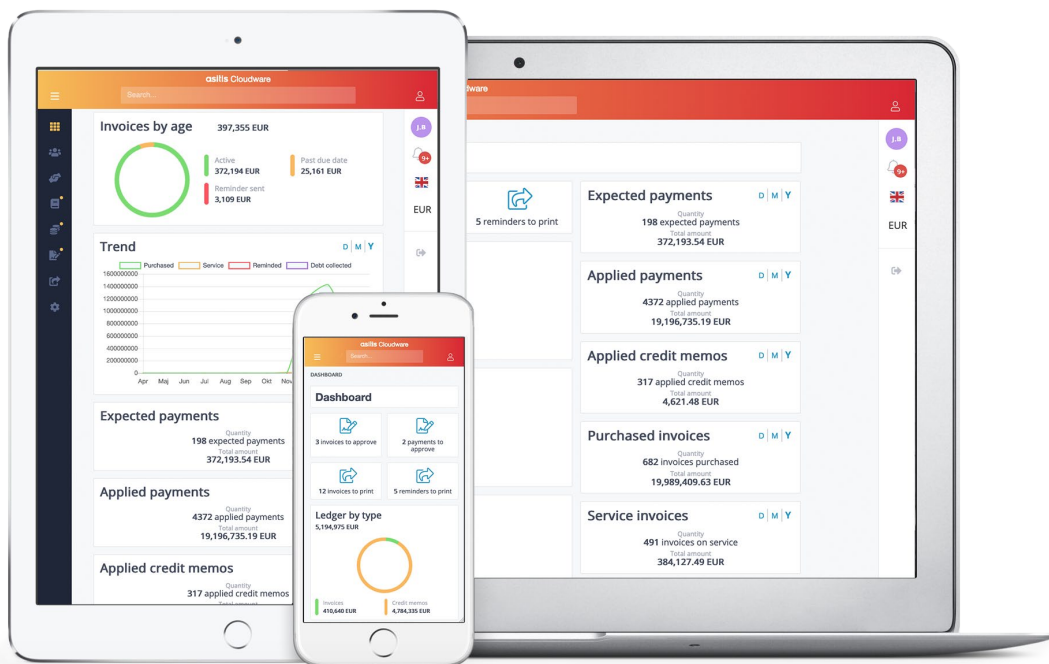
A high degree of self-service at all levels, as well as automation of previously manual tasks, raise productivity, reduce the risk of errors and create a positive customer experience.



Integrations and Microsoft Azure

Cloudware can easily be integrated with other services through defined and documented APIs. Cloudware is developed in Microsoft Azure. We apply proven technologies and methods in one of the world's leading cloud environments for safety and reliability. Azure's edge technologies continuously offer new tools and methods that help Asitis and our customers to be at the absolute edge of development.

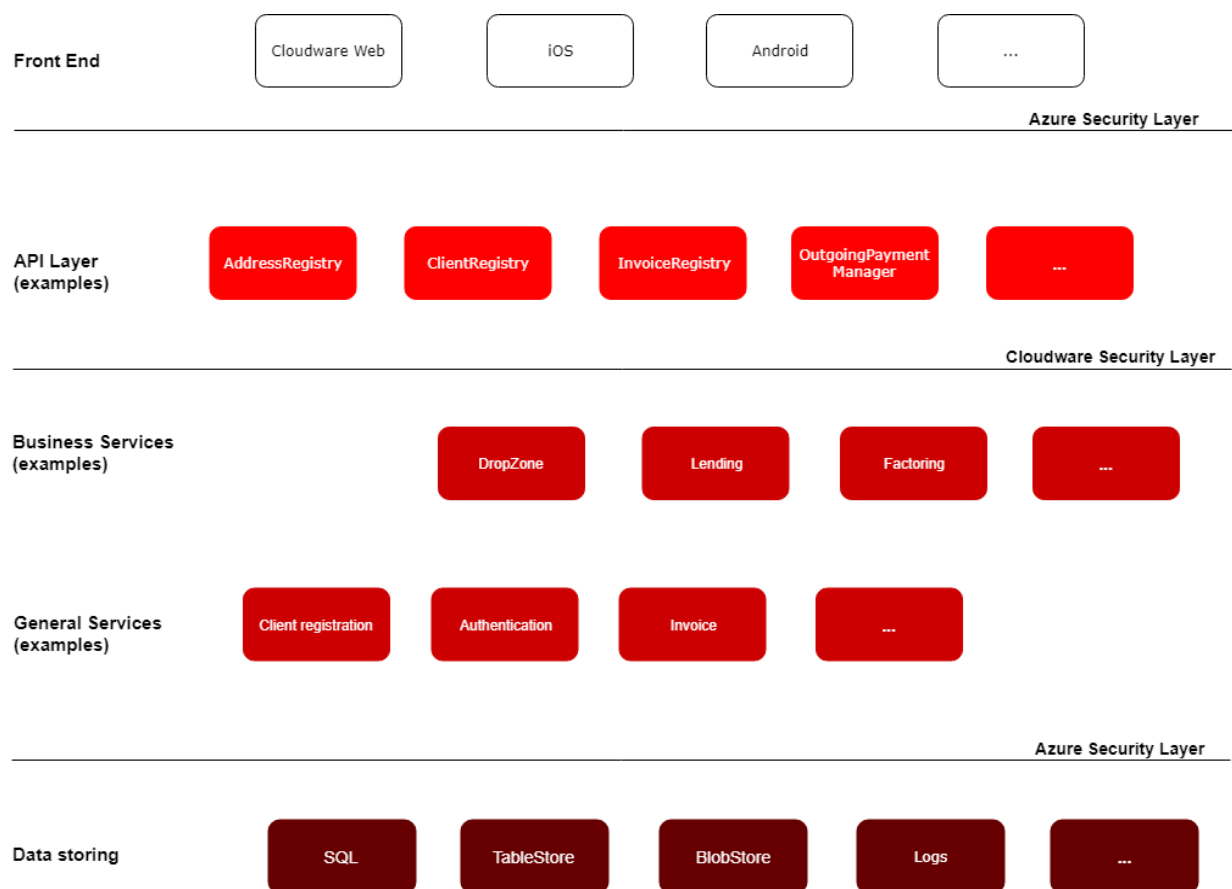
Cloudware is easy to on-board, to use and to grow with. The cloud-based solution in Microsoft Azure provides a secure and scalable service environment where you as a customer can focus on creating business value. Asitis takes responsibility for the server environment and further development required to meet your business needs.



2 Overall architecture

Asitis Cloudware constitutes the basis on which Asitis builds its future services and products, according to the market's needs and requirements. The development strategy is based on components where specialized micro services communicate with each other through APIs. This enables reuse of services and easy exchange of services. Once a base with general services has been created, they can be reused effectively - the development will thus be faster and faster for each new product being generated.

The service architecture is based on categorization of services, organized in different layers depending on the role and safety level of each service, as illustrated below.



Asitis Cloudware: Service layers

In the **front end layer** there are services for the graphical user interface. These are developed by Asitis but can easily be exchanged for other GUI services or via API communication integrated into existing external interfaces.

The API layer is the link between front end and back end. Communication through defined APIs in the API layer is the only way to exchange information with the Cloudware core. When in need of, for example, customization or integration with external products, specific APIs can be created.

Cloudware **security layer** governs API communications with *business services* and *general* Cloudware services based on roles and permissions.

The core of Cloudware consists of **business services / products** that create specific business values. Examples of these services are invoice purchase and DropZone. Furthermore, there are general features and services in the core, which are designed for existing, as well as future products in Cloudware. This layer can be divided over multiple machines if needed.

Azure Security Storage is a layer that secures the separation of all information at the database level.

For all **data storage**, the principle applies that data is stored as suitable for the data type and purpose. This means that we have a variety of databases for different purposes, which means that not all data is stored in one and the same SQL server. This is a crucial key to scalability.

2.1 Scaling

In the map of architecture mentioned above, we can scale in several areas:

- 1 Scaling in traffic volume**
- 2 Scaling in number of services in the business layer and in general services** - for example, the same service can be run in multiple copies on multiple machines, thus relieving the process flow.
- 3 Scaling at database level** - Already by dividing data by information type, classical data sources such as SQL Server are enormously relieved. For example, information can be divided over multiple machines depending on the data type, which provides amazing possibilities for Azure to balance the work load.
- 4 Scaling in working methods** - A crucial key to scaling lies in how information is processed in Cloudware. Instead of handling data in batches, each operation is handled according to a queue system. Scaling in Cloudware means several services working with the same tasks in order to shorten the existing queue with tasks.

2.2 Backup

Information in Azure is stored using *geo redundant*, which means that backup information is securely stored on one or more secondary sites to fully manage *full disaster events*. As with a common local SQL server, Azure allows you to control how often backups run and are stored. It is also possible to have one or more secondary sites available in real time for reading information in a worst-case scenario.

The following article provides more information about Azure backups, and how to manage the cleanup of GDPR sensitive information in backups.

<https://docs.microsoft.com/en-us/azure/sql-database/sql-database-automated-backups>

Encryption of data and backups

Azure has encryption of databases as well as backups by default. It requires an active choice to remove the encryption.

In conclusion, Cloudware and Azure offer the solutions you need in order to meet the requirements that your organization imposes on encryption of information as well as backup of and availability to information.

3 Development, testing and testing tools

How development, testing, and testing tools work in a project, is often a big issue. The Cloudware development process consists of several steps in which Asitis in each part has an appointed *responsible person* who ensures that the outcome corresponds to the required result.

1. Development environment

The *developer* is responsible for individual testing during the development process. Development takes place in a development environment, and when the developer is ready, a release of the functionality is made into an internal test environment.

2. Internal test environment

In the internal test environment, the *Scrum master* is responsible for the functionality being consistent with the requirements in the "user story". When the *Scrum master* gives its ok on functionality and any other functionality that has been affected by the development, the *scrum master* hands over to the *product owner*

who, in turn, tests the functionality. When the product owner approves, a release of the functionality is made to the acceptance test environment.

3. Acceptance test

Acceptance tests include sample tests as well as overall tests, performed by a dedicated *test team*. Once these functionality tests are done, the test team approves the release to the next instance. This next instance may be a customer dedicated test system, if it concerns customer-specific functionality. General functionality may be approved to be directly released into production.

Automated tests

In parallel to the above-mentioned tests, automated tests also take place in form of integration tests. These are developed in conjunction with the ongoing development. This means that integration tests are continually testing APIs and other vital functionality, delivering real-time results. You can follow the status of the integration tests in one dashboard - per environment.

Since the project started, Asitis Cloudware has had a background process in place, which continuously creates test invoices, payments, credits, credit invoices and so on. This ensures that Asitis environments contain live test data and that simultaneously ongoing testing of our APIs, as well as performance, are made. The background process currently creates about 20,000 invoices, 10,000 payments and a few thousand credit invoices each night.

4 API-information – Azure API Management

Azure Portal contains tools to easily provide a clear overview of available APIs per environment. It is possible for you to create your own accounts in Azure Portal. Asitis sales representative / account manager can assist you with this.

In addition to obtaining information about an API design, there are ongoing statistics about the usage of the API, such as number of calls, incoming data quantity, outgoing data quantity, and average response time. This information is available minute by minute in real time. It is also possible to track performance over time and diagnose possible problems as well as receive help to solve problems. There are ongoing logs and other useful

information. In combination with Application Insights (see below), it provides a good overview of available APIs, their functionality and health.

Below we can see an example of application services and web services running on various Azure service plans. Upon closer inspection of the image, we can state that the services are run in the development environment, the test environment, and the acceptance environment. We can also see examples of web services such as search, address register, and authorization management as well as web services that keep track of balance sheets in the economy.

NAME	STATUS	APP TYPE	APP SERVICE PLAN	LOCATION	SUBSCRIPTION
AddressRegistry-acc	Running	Web app	Acc-ServicePlan-1-S1	West Europe	AsitisFS AFS Dev
AddressRegistry-dev	Running	Web app	ServicePlan-1-S1	West Europe	AsitisFS AFS Dev
AddressRegistry-test	Running	Web app	Test-ServicePlan-1-S1	West Europe	AsitisFS AFS Dev
AFSearch-acc	Running	Web app	Acc-ServicePlan-1-S1	West Europe	AsitisFS AFS Dev
AFSearch-dev	Running	Web app	ServicePlan-1-S1	West Europe	AsitisFS AFS Dev
AFSearch-test	Running	Web app	Test-ServicePlan-1-S1	West Europe	AsitisFS AFS Dev
AsitisApiDoc	Running	Web app	ServicePlan-1-S1	West Europe	AsitisFS AFS Dev
AuthMaster-acc	Running	Web app	Acc-ServicePlan-1-S1	West Europe	AsitisFS AFS Dev
AuthMaster-dev	Running	Web app	ServicePlan-1-S1	West Europe	AsitisFS AFS Dev
AuthMaster-test	Running	Web app	Test-ServicePlan-1-S1	West Europe	AsitisFS AFS Dev
BalanceTransactionTracker-acc	Running	Web app	Acc-ServicePlan-1-S1	West Europe	AsitisFS AFS Dev
BalanceTransactionTracker-dev	Running	Web app	ServicePlan-1-S1	West Europe	AsitisFS AFS Dev
BalanceTransactionTracker-test	Running	Web app	Test-ServicePlan-1-S1	West Europe	AsitisFS AFS Dev
ClientFeeRegistry-acc	Running	Web app	Acc-ServicePlan-1-S1	West Europe	AsitisFS AFS Dev

Azure App-services

5 Security and Surveillance

Asitis uses all the security and surveillance systems offered by Azure. Azure's security layer guarantees that no unauthorized user can access the information they are not entitled to see. This security layer also guarantees that information cannot be shared between Asitis customers.

The information is stored in different tenants, and every single customer at Asitis is managed as a separate tenant, which has its own AD that controls the access.

In addition to this security layer, Asitis Cloudware has further separated the possibilities to access data, as described below.

5.1 Role based access system

The roles and rights are set through Asitis unique solution where we can create a hierarchy of access levels. There is no limit in Cloudware to how many levels the hierarchy can support.

Exampel of a simple hierarchy structure

- Finance company
 - Finance company clients
 - Client 1
 - Client 2
 - Client 2 – Department 1
 - Client 2 – Department 2
 - Department 2 – Economy
 - Department 2 – Substitute

This model symbolizes the hierarchical structure of a company and its customers. In addition, there are predefined roles per level where, for example, the financial director of the company is entitled to see all the information, including client data and its subdivisions. Thus, as a financial manager at the financial company, you have access to all information. The principle of an account manager at the client is the same but based on its level in the hierarchy. That person sees everything that concerns the client and its departments.

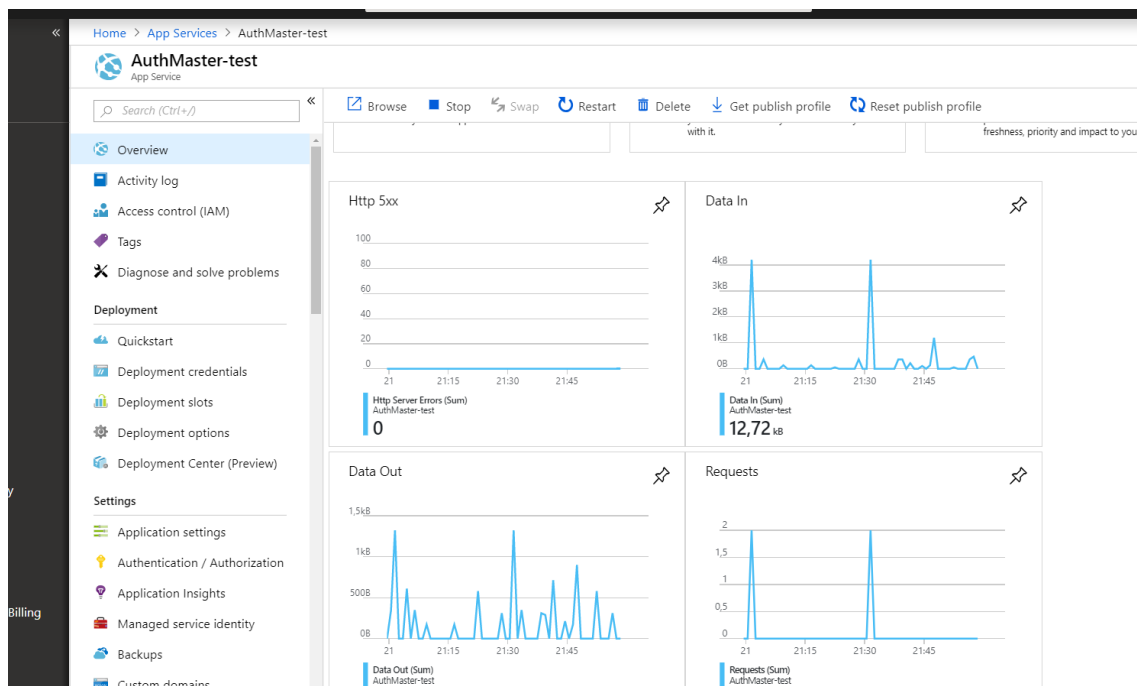
The hierarchy structure together with the defined role, determines what the user is entitled to see, which means that basically all functionality takes this into consideration. This way, the user cannot search or list information that the role does not permit. The exception can be, for example, export of information. A certain role may be granted to export invoices to debt collection even though it is not entitled to search for the invoices. All this can be defined in the permissions for the role.

In conclusion, Asitis Cloudware is based on the following:

- Azure AD
- Asitis Cloudware organization hierarchy
- Role-based permissions
- Persons connected to roles as above

As a note to the above, each subdivision in the hierarchy can be defined as a legal entity or department. In practice, this controls whether it is a business unit or not.

The print screen of the Azure portal below shows details of the service handling permissions in our test environment. The menu items show logs and settings while the graphs provide an overview of the health of the service and how it works.



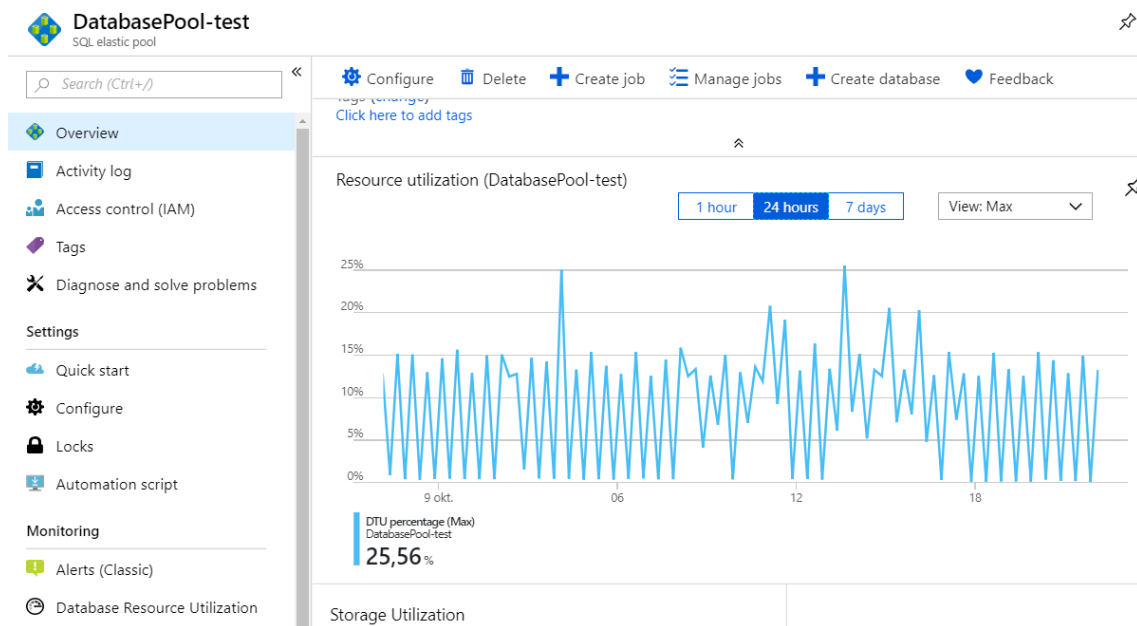
Azure Portal

5.2 Elastic Databases

Azure Elastic databases is a concept to provide the ability to utilize data storage media in the best possible way meanwhile providing a powerful scaling ability. The security of Elastic DB rests on the same permissions as Azure (AD) down to object level in the database. In this way, separation of different customers data is ensured.

Below is a print screen from Azure Portal showing the usage of a database pool in a test environment, and how it performs during a day. We can see that the use of the database pool dedicated to testing has exceeded 25% of the available capacity. Under the menu Storage Utilization, you can see that approximately 3% of the available database space is currently being used.

Of course, it is also possible to set limits for what is acceptable for both CPU utilization and utilization of space, which allows you to act in time to either increase performance or create more space.



Azure Portal: Database surveillance

5.3 Continuous development and continuous integration

The Asitis software development process is briefly described under the chapter "Testing and testing tools. One of the key factors to ensure a high-quality development process including both high speed and excellent quality is that the individual developer is obliged to make the release of its development to the internal test environment.

It is also the responsibility of the developer to maintain integration tests. If the developer fails to follow this, the integration tests instantly indicate this by showing a red light on the Asitis dashboard, and the error can be noted and corrected. This provides an additional incentive for the developer to take care of his commitments.

5.4 Azure monitoring tools

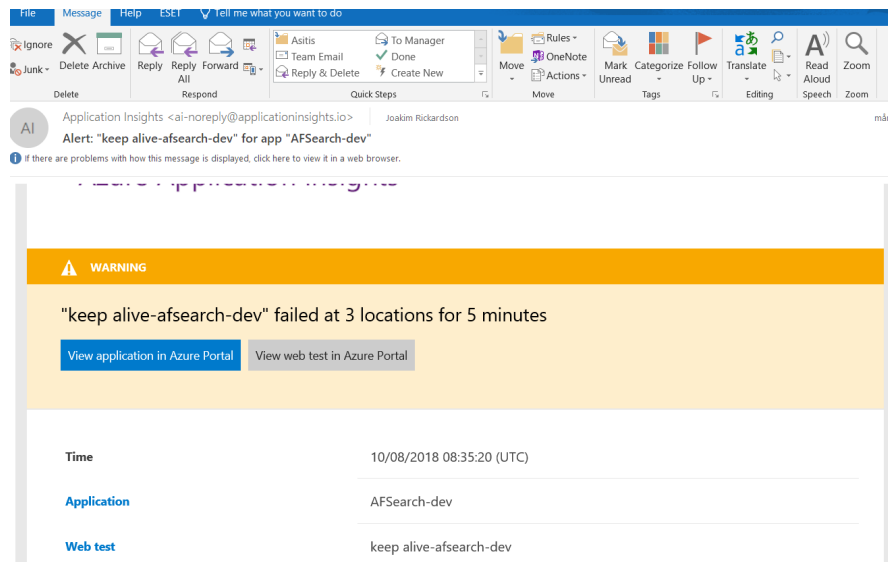
Azure offers a number of useful tools for monitoring and tracking, all accessible through the portal. The comprehensive network monitoring tools help you monitor your network performance, detect network faults in real time, troubleshoot errors, and prevent downtime. Parts of this are described above.

5.5 Azure Application insights

Application insights provide a number of different benefits, and one of the most interesting is the ongoing performance review. This insight notifies via email when a service performs poorly so the right kind of action can be taken. For example, a specific service can according to the estimation be performing well, but 10% worse than last week, an event that would require some attention.

Furthermore, you can get live information about available resources like CPU, disk space or data flow through the firewall. The goal is to react before it's too late and thus create a sense of security for the user that everything works as it should.

Below is an email notification from Application Insights informing the affected operating organization that the search function is not working in the development environment. Should it happen in a production environment, the affected operating organization receives prompt information, which means that it can immediately fix the problem.



Application Insights

5.6 Azure and network access

Asitis Cloudware uses firewall functionality, but also functionality for monitoring and balancing the work load. The solution is built to be scaled up in infinity where neither network, server capacity nor disk space will become a bottleneck. Azure also provides a live status of the organizations use of the network and status of the current capacity.

5.7 Compliance - Audit-logging of sensitive data

Asitis Cloudware logs information for several reasons. It can be a real audit logging, but also to create a basis for billing. *Cloudware* logs changes, but also when a user chooses to access specific information that is hidden by default. The user is entitled to view the current information, but it is logged that the user has made an active choice to view the information. This allows tracking of how different users take part of personal data.

5.8 Hybrid solutions

The possibility of hybrid integration is limitless in Cloudware. The entire Asitis Cloudware is built to support Asitis APIs, which means that data access can be made through APIs if the user has the right permission. There are also opportunities for integration with other solutions such as Asitis Finance or a data warehouse, which also makes it possible to build entirely customized interfaces or unique custom widgets. The customer can by thus build completely customized solutions for imports, exports, reports, and much more.

6 Contact

Please contact us to be presented with a live demo, to ask questions or get a quote.

Tel 0500-600 200 or by e-mail: hello@asitis.se

We look forward to hearing from you!