itelligence NTT DATA Business Solutions

SAP Commerce Cloud Support

Optimise your SAP Commerce Cloud Website with an itelligence Advanced Health Check

> With itelligence’s support, we can be confident that interruptions and downtime will be minimised, efficiencies are maintained, and customers enjoy the best possible experience of shopping online with us.”
>
> Rob WIlson, Chief Technology Officer, Smyths Toys

SAP Commerce Cloud Support

Optimise your SAP Commerce Cloud Website with an itelligence Advanced Health Check

Boost your E-Commerce Performance

Any enterprise e-commerce solution worth having will have a number of characteristics you cannot avoid, from the expense, time and effort to get the system up and running, to the need for constant monitoring. However get it right and you will reap the benefits of a modular, agile, end-to-end solution that creates a great customer experience, keeping customers coming back for more.

itelligence: Experts in E-Commerce Solutions

We understand the challenges faced by UK organisations in these unprecedented times and are working with many brands to ensure success in their e-commerce activities. As SAP and Customer Experience (CX) specialists we have developed our own e-commerce health check to ensure your SAP Commerce Cloud (formerly known as Hybris) platform is fully optimised to support your business objectives now and in the future.

Our Health Check Service

Our Advanced Health Check Service examines common problems with an e-commerce website and includes a comprehensive review of the platform’s performance, security & compliance, resilience and user experience.

Key Benefits of our SAP Commerce Cloud Health Check:

- In-depth report identifying potential optimisations
- Remote assessment
- Personalised appraisals for improvement
- 360 degree view into your SAP investment
- Analysis to drive better conversions and AOV

3 weeks on average for an Advanced SAP Commerce Cloud Health Check

The Advanced SAP Commerce Cloud Health Check includes everything contained in the Standard SAP Commerce Cloud Health Check, plus the following:

Best Practices

Webroot

We will check that the webroot of your application is correctly set to / and that HAC has been moved to /hac or /admin.

HTTP Proxy Timeout

We will check that the application session timeout is lower than the sticky session timeout to ensure sessions are not lost.

Virtual Hosts

If you have more than one storefront, we will check that virtual hosts are set up correctly at the CDN or web tier and that the correct redirects exist for the relevant host headers.

Application Server Node Session Failover

We will check that cart contents are restored when an application server fails and the user is redirected to a different application server.

Error Pages

We will check that branded error pages for 403, 404 and 500 HTTP errors are configured in the storefront application and for 502, 503 and 504 are configured at the CDN or web tier.

Full HTTP Session Replication

We will check if full HTTP session replication is configured to ensure user login preservation in case of persistence loss. This is configured at the CDN or web tier.

Java TimeZones

We will check if the Java TimeZone is set to the same value on all SAP Commerce Cloud servers, and that this matches the database TimeZone.

Language Settings

We will check if the language settings LANG and LC_* are correct.

Licensing

We will check that each environment has its specific license defined in local.properties and each points to the correct license file.

SEO Redirects

If you have migrated to SAP Commerce Cloud from an existing website recently, we will check that your SEO redirects are correctly set up.

Operations

Log Aggregation

We will check your logging setup to make sure all logs are held centrally in a log aggregator such as Logstash or Splunk.

Runtime Log Changes

We will check you can alter log levels at runtime for certain classes where it may be necessary to do so.

Default Log Levels

We will check your logging setup to make sure the minimum productive log level is set to WARN or higher.

Monitoring

We will check your monitoring setup to make sure the right people receive the right monitoring alerts and that a structure is in place for tackling known errors.

System Observability

All systems must always be observable by the operations team to allow for complete system monitoring and allow problems to be resolved quickly and efficiently. We will review your system architecture to ensure that this is the case.

Performance

Sticky Sessions
We will check if sticky sessions are correctly configured on your application server load balancer.

Maintenance Pages
We will check that maintenance pages are configured at the CDN or web tier.

Favicon
We will check that a favicon is correctly defined for the web application at the CDN or web tier.

Compression
We will check that compression is correctly configured at the CDN or web tier.

Client Profiling
We will check that all client profiling items are addressed, including combining and minifying CSS and JavaScript, deferring JavaScript loading, minimising the number of resources on a page and using effective cache headers.

Java Garbage Collection
We will check your Java garbage collection settings to make sure they are in-line with SAP Commerce Cloud recommendations.

Performance Properties
We will check that the relevant performance properties for Tomcat, Catalog Sync, Impex Import Workers and the CMS Cache are set.

Advanced Personalisation
We will check that Advanced Personalisation is disabled if it is not required.

Session Timeout
We will check that session timeout values are set to appropriate values.

Database Pool Settings
We will check that the database pool settings are appropriate for the environment.

Catalog Sync Process
We will check that the catalog sync process has been appropriately tuned.

Lucene Cron Jobs
We will check that the Lucene cron jobs have been disabled.

Price Accuracy
We will check that the price accuracy has been set per your requirements.

SAP Commerce Cloud Cache Size Tuning
We will check that SAP Commerce Cloud Cache sizes have been appropriately tuned.

Index Definition
We will check that the necessary indexes for custom types and attributes exist in the database.

Deployment and Sync Under Load
We will check that the deployment and sync processes work correctly and do not negatively affect storefront performance when the customer-facing site is under heavy load.

HMC Case Sensitive Search
We will check that case sensitive searching is disabled in HMC.

Packet Collisions
We will check that packet collisions are not excessive.

Database Table Maintenance
We will review your database table maintenance procedures to ensure that you have a process to deal with excessive table growth.

3 weeks
on average for an Advanced SAP Commerce Cloud Health Check

NIC Saturation

We will check that NICs are not reaching bandwidth saturation.

DNS TTL

We will check that the TTL for the DNS record for the customer-facing site is not excessively high.

Autoscaling

We will review your system architecture to ensure that your system is capable of automatically scaling in response to changes in demand.

Resilience

Backup and Restore Strategy

We will check if the backup and restore strategy meets your defined SLAs and review your previous tests of this process.

Deployment Process

We will check your deployment process to make sure that it is stable, well documented, tested and repeatable.

Hardware Support

We will check that the hardware on which SAP Commerce Cloud is running is supported according to the environments matrix.

Task Engine and Cron Jobs

We will check that the task engine and cron jobs do not run on storefront nodes.

Disaster Recovery

We will review your disaster recovery procedures are appropriate according to your SLAs and requirements.

Initialisation and Update

We will check that initialisation and update screens in HAC are disabled and that system unlocking is disabled in the production environment.

Shared Resources

We will review your system architecture to ensure that any shared resources accessed by more than one SAP Commerce Cloud application server are not a single point of failure.

OS-Level Tasks

We will review your system architecture to ensure that any tasks performed at the operating system level do not constitute a single point of failure.

Auto-healing

We will review your system architecture to ensure that your system is capable of automatically healing itself in response to detected system failures.

Unit Tests

We will review your source code to ensure maximum coverage of custom extensions by unit tests.

Automated Tests

We will review your deployment pipeline to ensure all your specifications are covered by automated tests.

Stress Tests

We will review your testing procedure to ensure your application passes stress tests based on your specifications. Stress tests measure the maximum capacity of the website.

Spike Tests

We will review your testing procedure to ensure your application passes spike tests based on your specifications. Spike tests measure the SAP Commerce Cloud website's response to a sudden jump in traffic.

Soak Tests

We will review your testing procedure to ensure your application passes soak tests based on your specifications. Soak tests measure the SAP Commerce Cloud website's ability to sustain high load for an extended period.

Security

Proxy Rules

As well as the proxy rules required to block the 130 standard webroots, we will check that any custom extensions are also blocked by proxy rules.

HTTPS Spring Security Configuration

We will review spring-security-config.xml to ensure the spring security rules enforce all storefront web applications run under HTTPS.

Directory Listing

We will check if directory listing is disabled at the web and application tiers.

Sensitive Data

We will check your SAP Commerce Cloud code to ensure that sensitive data, such as credit card numbers or other personally identifiable information, is not revealed in log files.

JDK Version

We will check your JDK version is supported by SAP Commerce Cloud and that you have a process to upgrade monthly to the latest security patches.

SAP Commerce Cloud Version

We will check the version of SAP Commerce Cloud is the latest patch level to ensure you do not have known security flaws and that you have a process to upgrade monthly to the latest patch level.

SSL Certificates

We will check your SSL certificate issuance and distribution process to ensure that you are using valid certificates with the proper domain and that you are not at risk of private key leakage.

SAP Commerce Cloud Cluster Settings

We will check that there is network separation between environments and that each environment uses a unique JGroups channel.

Unused Extensions

We will check that any unused extensions are removed from the build process.

SAP Commerce Cloud Development Settings

We will check that SAP Commerce Cloud development settings are disabled in the production environment.

Password Security

We will check that password hashing uses at least SHA256 and that the default salt value is not in use.

Password Encoding

We will check that all users' and customers' passwords were hashed with at least SHA256.

Item Change History

We will check that the history of changes to items is recorded appropriately in the production environment.

Default Passwords

We will check that the default passwords for all employees have been changed and that administrative and default users do not have default passwords.

Transparent Attribute Encryption

We will check that the default master password and encryption key for transparent attribute encryption have been changed.

Web Application Firewall

We will check that a Web Application Firewall (WAF) is in place and appropriately configured.

3 weeks on average for an Advanced SAP Commerce Cloud Health Check

SAP Commerce Cloud OS User

We will check that SAP Commerce Cloud is not running as the OS root user.

JMX Security

We will check that the appropriate JMX security settings are correctly configured.

OS Patching

We will review your operating system patching procedures to ensure you have a process to fix known vulnerabilities every month.

Role Separation

We will review your system architecture to ensure that SAP Commerce Cloud storefront and backend servers, and Solr master and slave servers, are not running on the same OS.

Source Code Analysis

We will review your source code to detect known vulnerabilities, inefficiencies, duplication and other common problems.

Solr Version

We will check the version of Solr is the latest patch level to ensure you do not have known security flaws and that you have a process to upgrade monthly to the latest patch level.

Firewall Rules

We will review your firewall rules to ensure that they sufficiently restrict access to your landscape.

Data Encryption

We will review your system architecture to ensure that all data is encrypted at rest and in transit.

Secret Security

We will review your code and system architecture to ensure that secrets – passwords, private keys and the like – are stored in secret storage and are accessible only by runtime components.

Access Requirements

We will need read access to your entire landscape to be able to check that everything is set up correctly and that your procedures meet your operational requirements and SLAs.

Application Code

We will need read access to your application code. This is commonly a git repository, but may be using other technologies.

Integration Tools

We will need read access to the integration tools you use for application deployment and delivery. This is commonly GitLab, Jenkins or some other CI/CD build tool, but may use other technologies.

Application Servers

We will need read access to the administrative tools of your SAP Commerce Cloud application servers – BackOffice, HAC and so on. We will also need read access at the OS or container level. We will also need read access to the administrative layer and underlying OS of your Solr application servers.

Web Servers

We will need read access to your web servers. This will depend on what type of web server you are using. It may be SSH access, RDP access, or management application access.

CDN

We will need read access to your CDN, including access to both configuration and logs.

Load Balancer

We will need read access to your load balancer, including access to both configuration and logs.

DNS

We will need read access to your DNS, to check the records are set up correctly.

Database

We will need read access to your database, at both the database level and, if it is not a managed service, at the OS level. If it is a managed service, we will require access to management tools.

Network Layer

We will need read access to your network devices, to check things like traffic saturation, firewall rules, network separation and access control lists.

Cloud, Container or VM Platform

We will need read access to your cloud, container or VM platform, to check how your application is configured to scale in response to demand.

Hardware

If you are using on-premise or co-located hardware, we will need access to this so that we can check its compatibility with SAP Commerce Cloud and Solr, and to ensure that appropriate procedures surrounding things like firmware updates are in place.

SSL Certificate Provider

We will need read access to your SSL certificate provider, to check your issuance process is not susceptible to private key loss and other potential vulnerabilities.

Web Application Firewall

We will need read access to your web application firewall, to check its configuration and that rules are in place to mitigate known web application vulnerabilities.

Storage

We will need read access to your storage subsystem, to check encryption settings and I/O configuration.

Secret Storage

We will need read access to your secret storage configuration so that we can check the appropriate access controls and security measures are in place.

Backup Systems

We will need read access to your backup systems so that we can check your backup and restore procedures are correct.

Monitoring

We will need read access to your monitoring systems so that we can check the correct things are being monitored and actions exist based on trigger levels or states.

Procedures

We will need to see your deployment, backup, recovery, database table maintenance, OS, application and hardware patching, disaster recovery, stress test, spike test, soak test, log review and monitoring procedures to ensure that they are fit for purpose.

SLAs

We will need to see your SLAs so that we can check that the above procedures meet the operational requirements that you will need to fulfil them.

Contact us to today to learn more:

» info@itelligencegroup.co.uk
» www.itelligencegroup.com