KP audit “___”

1. Site verification using standard 1C-Bitrix tools

1.1. Testing the configuration

No errors were detected.

Comments:

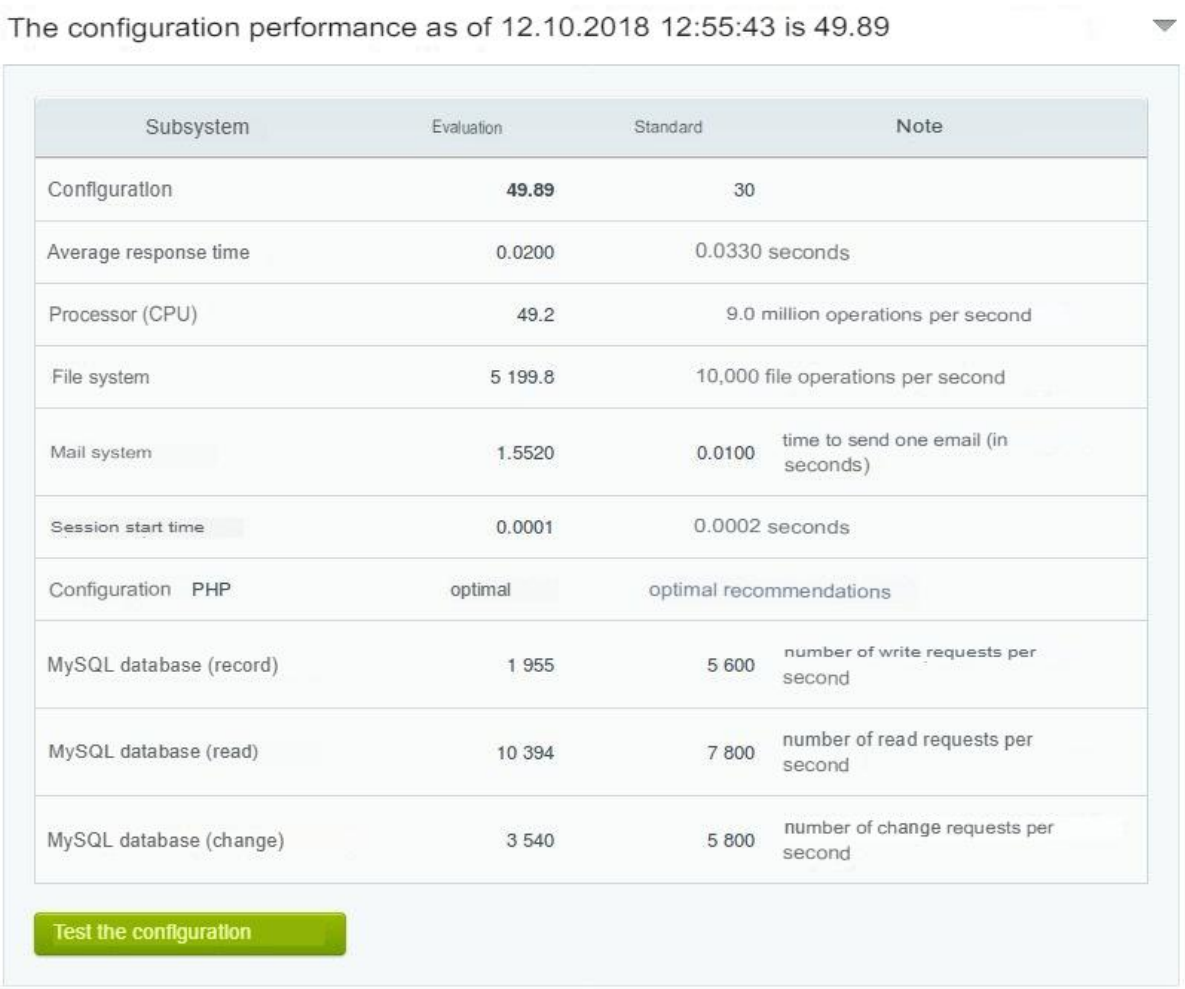
1. Sending mail - delivered. Sending time: 1.51 seconds.

2. Sending an email message larger than 64Kb - delivered. Sending time: 2.37 seconds.

The time is acceptable, but slightly longer than the ideal time for Bitrix.

Testing the configuration

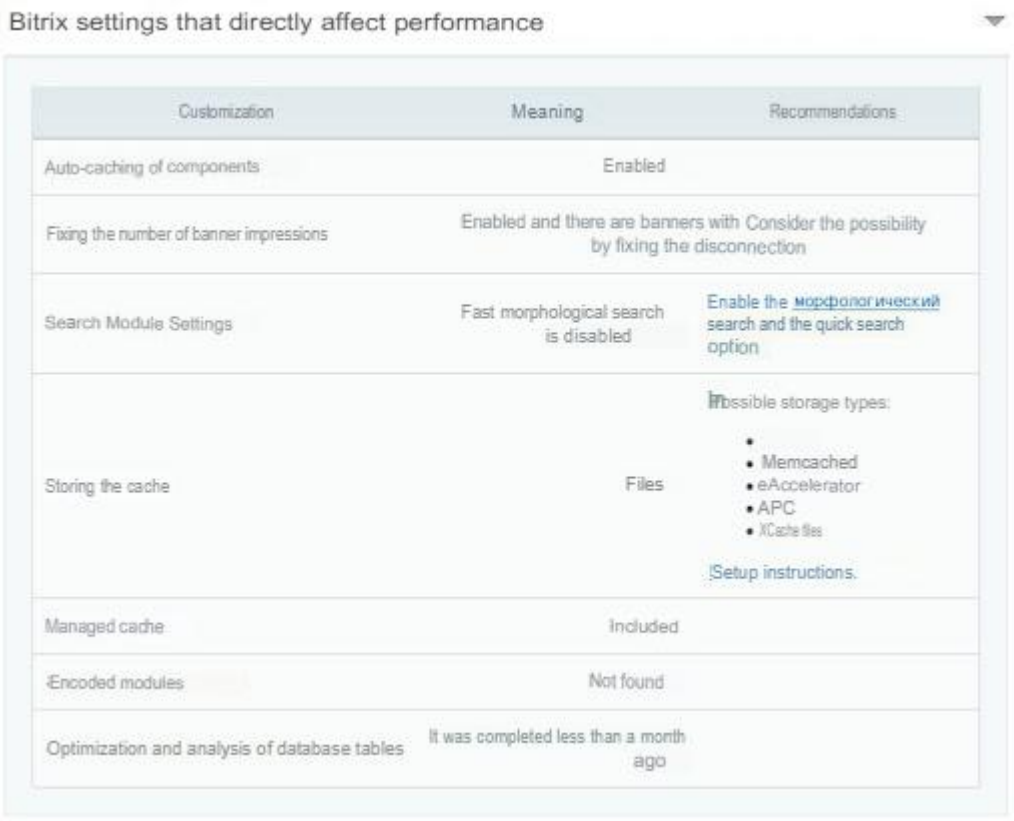
The server configuration generally meets the requirements.



Web Server and Software Configuration

We recommend disabling banner fixing. This option can be useful for websites.
There are no ads in the corporate portal, so you don't need to fix the display of banners.

Fast morphological search is disabled. For faster search, we recommend installing the Sphinx search engine. Using Sphinx as a search engine will significantly increase the search speed and reduce server load. Since you are using a 7.3.2 VM, you can install Sphinx via the VM. Reindexing and changing the search engine to Sphinx will happen automatically.

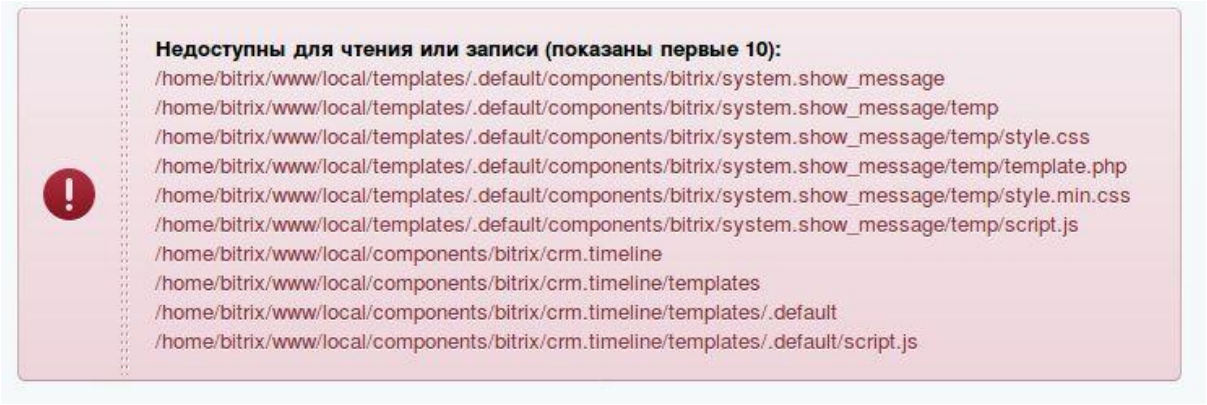


1.2. Testing the site's speed.

Performance testing was performed (in 1 hour, more than 1,100 requests were sent).
The query execution time is within the normal range, and there are no abnormally long requests.
The page execution time does not exceed 3 seconds.

1.3. Access verification.

More than 10 files cannot be read or written.



Recommendation: set the correct file permissions. The owner must be “bitrix”. Set file permissions to 664 and folder permissions to 755.

1.4. Portal backup.

Automatic backup is enabled. Backups are created normally, and there are no errors in the backup log.

1.5. SSL.

The certificate is configured correctly. “Regular dehydrated” is used

.

1.6. Security scanner.

Service files were found.
File /home/bitrix/www/mysql_debug. sql.
Recommendation:
Delete the file or restrict access to them correctly.
With the current settings, an attacker can download a database backup by clicking on the link ___/mysql_debug. sql

The security level of the administrative group is not increased.
Recommendation:
Our advice is to increase the level of security from “elementary” to “advanced.
To do this, go to “Edit Admin group (id=1)”. In the “Security” tab, in the “Predefined security level settings” field, set the value = “Advanced”.

Advanced error output is enabled.
Recommendation:
We don’t advise to display the error text. It is recommended to change the "debug" parameter in the configuration file /home/bitrix/www/bitrix/.settings.php.

Detected at least 6 files or directories with write access for all users of the web server environment.

/bitrix/activities/custom/crmgetdataentityactivity
/bitrix/activities/custom/crmgetdataentityactivity/crmgetdataentityactivity.php
/bitrix/activities/custom/crmgetdataentityactivity/lang
/bitrix/activities/custom/crmgetdataentityactivity/lang/en
/bitrix/activities/custom/crmgetdataentityactivity/lang/en/.description.php

Recommendation:
Change access rights to files and folders. Set file permissions to 664 and folder permissions to 755.

1.7. Web antivirus.

Recommendation:
Enable Web antivirus (Administrative Panel - > Proactive Protection ->Web antivirus) for better security.
You should also change the PHP configuration so that the file /home/bitrix/www/bitrix/modules/security/tools/start.php can detect viruses before output buffering starts.
To do this, add an entry auto_prepend_file = /home/bitrix/www/bitrix/modules/security/tools/start.php in the /etc/php.ini file and restart the Apache web server.

1.8. Frame protection.

Recommendation:
Enable frame protection (Admin Panel - > Proactive Protection - > Frame Protection) to prevent certain types of attacks (Clickjacking, Frame Sniffing).
You don't need to enable this option if you plan to use open lines. At the moment, an open line exists, but for the entire time of its existence, there has not been a single request, meaning, the open line is not in use.

2. Audit of improvements to the portal.

2.1. Electronic Document management and REGISTRY, dismissal of employees.

Business Process for "task transfer of a dismissed employee"
There’s an Extra variable "FirstEmp_id", which is always empty.
It contains an entry {=Document:PROPERTY_OT_KOGO_ID}. But prefixing” _ID " to the document field doesn't return anything.
If you start a business process, a notification appears. The link is created incorrectly - when clicked, the user is redirected to the site map.
You should change the link formation in the business process action.

The “delegate” function will never be called during PHP Code action.
MWIDelegateFired::DelegateAll($FirstEmp,$SecondEmp);
since this function is executed only if FirstEmp_id is not empty. And FirstEmp_id is always empty (see above). In other words, there will be no transfer of tasks.

2.2.Kanban.

The customer reported that the kanban revision is not yet complete. From the user's point of view, it is now possible to filter by department. Filtering works normally.

2.3. Records when deleting tasks.

The customization was made by subscribing to the delete task event. Recording takes place in the infoblock “INTEGRATION - Record to be deleted from the entity”, the id of the deleted task is saved, and the user who deleted it.
There are no comments.

2.4. Auto-tasks.

The customization was made using the mechanism - Bitrix Robots. If the created lead has a responsible person - "Mr. Bitrix", and the lead source is “Website", then a task is created. This logic works correctly.

Comments:
1. There are unused variables (for example, “Our Lead or partner's Lead"), and empty blocks ("Add more tasks").
2. The business process has some logic with a condition for execution that the lead id is equal to 0. Since the value of the created entity is always greater than 0, then this block will never be executed.

2.5. Pulling fields into deals.

Deals are updated in init.php depending on several conditions, for example, on the condition that a lead is updated. Implemented by subscribing to events.
There are no comments.

2.6. Required comments in tasks.

Implemented using JS (/local/lib/js/additional.js). This script tries to output “You didn't

save a comment” when an employee leaves the Business process task page, if the text in the comment is present, but the Save button was not clicked.
Note: You can set a mandatory comment in the BP settings. We recommend using the built-in "mandatory comment" feature.

2.7. Mandatory reasons for refusal

Updating Bitrix's pop-up via JS (/local/lib/js/additional.js). A positive result is removed from the list of lead statuses, and a negative result is selected programmatically. Added a text field for the reason for refusal. When you click Save, ajax is sent.

Remark:
1. The session id is not passed in the ajax request in this JS file, for example, on line 145. And accordingly, there is no verification on the server, which creates a vulnerability: a CSRF attack is possible.

2. Regarding negative stages in kanban. Currently not allowed in kanban lead move it to the negative stage. Stages are hidden from the user using css (/local/lib/css/additional.css).

2.8. Configuring backup to the microsoft onedrive cloud.

There is cron task for backup using duplicate:
0 3 * * * /usr/bin/duply ubitrix backup_verify_purge --force >> /var/log/duply.log 2>&1; /usr/bin/duply etc backup_verify_purge --force >> /var/log/duply.log 2>&1; /usr/bin/duply b24 backup_verify_purge --force >> /var/log/duply.log 2>&1
There are no errors in the /var/log/duplicate.log logs.

2.9. Backup of Lead files; Required fields in the lead; Creation of deals from the Lead.

Backup of Lead files.
The customer doesn't remember exactly what was meant by this revision. While investigating the code, the SaveAllLeadFiles (/) function was discovered local/php_interface/init.php).
Custom fields of the File type are saved. Since the lead doesn't have any fields of this type, no backup is performed.

Remark:
The CCrmLead::GetListEx selection uses the $SelectedFiles variable. There is no check for the emptiness of this variable. Because of this, all fields are selected, which was not intended.

Required fields in leads
The customization was made using the Bitrix Robots mechanism. Assigning a task to a responsible person, if the required fields are not filled in. However, this logic is executed only if the lead id = 0.
Since the id of the created lead cannot be set to 0, the task is never assigned to the responsible person.
The customer said that this customization will be removed in the near future.

Creating deals from a Lead
The revision was made through the Bitrix Robots mechanism. Creating a transaction to change the lead's stage.
A transaction is created only if the transaction id is 0. Since the id of the created lead cannot be equal to 0, the transaction is not created. The customer informed that the revision will be removed in the future.

2.10. Create personalized messages in the "Company" section.

The customer doesn't know what this revision is for. From the user's point of view, They did not notice the ability to create personalized messages in “companies” section.

2.11. Color new leads green ; Prepare the product field (new field) for the frame; Pull all fields from the lead to the deal card; Partner ID in the product.

Color new leads green
Using JS. If the lead name contains“$”, then the lead string is colored.
From the lead, all fields must be pulled to the transaction card
The OnAfterCrmLeadUpdate event is used. For each lead update, the linked deal is updated.
Note: Data loss may occur. If a field is updated in a deal, it may be overwritten later when the lead is updated.
Partner ID in the product
The CheckLeadProducts function is responsible for defining a feature in a product. init.php.
Note: in the checks below, the unit will never be returned.

```
if(in_array (1, $product_types) && in_array (2, $product_types))
return 3;
elseif(in_array (2, $product_types))
return 2;
elseif(in_array (2, $product_types))
return 1;
```

Prepare the product field (new field) for the frame
In the product saving function AfterProductRowsSave:

```
$entity = new CCrmLead(false);
$entity->update($ID, $fields);
$fields = array('UF_CRM_1529675483'=> true);
$entity = new CCrmLead(false);
$entity->update($ID, $fields);
```

It is advisable to not load the database with queries, if this can be avoided, in order to increase the performance of the portal. In this case, it is better to collect all the changes in one array, and then perform an update.

The customer reported that work on the goods management unit was suspended. At the moment, we can see improvements in adding a new tab to the lead detail page by modifying the crm.lead.details component (see below).

Note: There is a dependency on the user field UF_CRM_PRODUCT_TAB. Since this field does not exist, the tab will not be added.

2.12. Automatic creation of deals based on the attribute.

See “Creating deals from a Lead " above.

2.13. Other information.

Log file Availability

Any unauthorized user can read the logs at: ___/local/log.txt

Recommendation: change the logging method, or restrict access to the file.

Copying kernel files

Some third-party improvements (such as Kanban tasks) are based on copying Bitrix kernel files, and adding new functionality to them. Some templates, components, and the tasks modules were copied. What does this mean? When updating the portal, Bitrix changes the core files. However, the new

Bitrix functionality may not work during updates, as it will execute

outdated copied kernel files. Thus, when updating the portal, errors may appear that may take a very long time to fix.

Recommendation:

do not copy kernel files. Use other methods of customization: result_modifier and calling the original template, using JavaScript, and others.

Customer's question: “How much has the native bitrix php code been changed? How big is the chance that module updates will crash or faill?”

12 components, 6 templates, and 1 module were copied. This is quite a lot. Update failures will depend on the Bitrix updates themselves. If updates involve copied kernel files, crashes are almost inevitable.

At best, the new Bitrix functionality will simply not be visible.

{"mode":"full","isActive":false}