Zylinc
LIBERATING

Monitor the operational status of a Zylinc solution

www.zylinc.com

Monitor the operational status of a Zylinc solution

The information is this guide is for audiences with a technical background.

Many organizations want to be able to monitor how their critical IT and communications solutions perform, so that they can quickly deal with any potential problems before many users become affected.

If you work in IT operations or a similar function, this guide explains what you need to know if you're going to monitor the operational status of a Zylinc solution.

Monitor NTP service health

A Zylinc backend system basically has two parts: a Windows part and a Linux part.

The Zylinc Windows Application Server is the server that runs the Windows-based parts of the Zylinc solution.

The Zylinc Media Server is the server that runs the Debian Linux-based part of the Zylinc solution. The Media Server answers calls to queues, plays music on hold, makes interactive voice response menus work, etc. The Media Server also hosts the browser-based Zylinc Administration Portal in a Tomcat service that runs on the Linux operating system.

Correct time synchronization is critical on both the Windows Application Server and the Media Server. That's why it's a very good idea to monitor that time synchronization works as expected.

Monitor time synchronization on Windows

On Windows, time synchronization is usually handled as a part of the domain membership, and event log errors are available when you need to monitor the state of the time synchronization service.

For instructions about how to monitor time synchronization, refer to the documentation for your operating system and monitoring tool.

Monitor time synchronization on Zylinc Media Server

On the Linux-based Media Server, time synchronization relies on internal or external NTP (Network Time Protocol) servers.

Because you can’t monitor the Linux NTP daemon status directly on the Media Server, we recommend that you monitor the state of the NTP servers that you use.

For instructions about how to monitor the state of NTP servers, refer to the documentation for your monitoring tool.

Monitor SQL Server availability

A Zylinc solution has two important SQL Server databases, called ZyDB and ZyStatDB.

The installation guidelines for a typical Zylinc solution describe how to install and set up Microsoft SQL Server Express as a service that's located on the same server that hosts the rest of the Zylinc solution's Windows-based software.

You can also use other editions of SQL Server, like Standard or Enterprise edition, and you can also choose to install SQL Server on a dedicated server or cluster.

Monitor SQL Server service

We recommend that you monitor the SQL Server service. It doesn't matter if it's located on the same server as the rest of the Windows services, or if you use an external server or cluster to host the service.

Proactively monitor disk usage of SQL Server

One of the most common issues that can cause your Zylinc solution to become unavailable to the users in your organization is if a database runs out of available space and becomes read-only.

If you want to proactively prevent this, we recommend that you keep an eye on the following:

- Monitor that all disks in your SQL server always have a reasonable amount of free space available, *for example* at least 5 GB of available space per disk.
- Check **recovery model** and *backup schedule* for all your databases, as described in the following:

Manually check database recovery models and backup schedules

If your backup schedule doesn't include a regular transaction log backup, and **Recovery model** for a database is set to **Full** or **Bulk-logged**, the database transaction log files (LDF files) will expand until the disk is full. The database will become read-only and your Zylinc solution will become unavailable. We don't want that!

You can use SQL Server Management Studio to go through all your databases and manually check the **Recovery model** for each of them. If you find a database that has its **Recovery model** set to **Full** or **Bulk-logged**, you should then check if the **Last Database Log Backup** is not too old, for example, older than 24 hours.

The advantage of frequent log backups is that they increase the frequency of log truncation, which results in smaller log files. That's why, if the **Last Database Log Backup** is not too old, you can assume, with a high degree of certainty, that a backup schedule includes a regular transaction log backup for that database, which in turn indicates that your configuration is OK.

However, there's an easier way: Automatically check your configuration with the SQL script that we describe in the following.

SQL script to check database recovery models and backup schedules

1. Start SQL Server Management Studio and connect to the SQL Server that hosts ZyDB.
2. Click **New Query**.
3. Copy the SQL code from the topic *Monitor SQL Server availability* on Zylinc unified help.

4. Optionally, edit the first line of the script. The default value for the oldest accepted age of a backup is 24 hours (24*60 minutes). If you want, you can change that value to something else.

   For example, to extend the value to 7 days, change the line to:

   ```
   DECLARE @max_allowed_backup_age_in_minutes_before_warning INT =
   7*24*60
   ```

5. Press F5 or click **Execute** to run the script.

6. If the script doesn't return any warnings in the **TestCase** or **TestResult** columns, your recovery model and backup schedule configuration is likely to be OK.

If there's a potential problem, the script can return any of these four warnings for each of the user-databases on your SQL server:

TestCase	TestResult
490 No backup for "<database name>": According to MSDB backup history, this database has never been backed up.	Info/Warning
500 Backup too old for "<database name>": According to MSDB backup history, the most recent backup for this database is too old (older than <minutes> minutes).	Info/Warning
510 No transaction log backup for "<database name>". Risk of disk full in the future: There is a risk that the database transaction log files (LDF files) for this database will expand until the disk is full. The recovery model for this database is set to "FULL" or "BULK_LOGGED" but according to MSDB backup history, the transaction log has never been backed up.	Info/Warning
520 Transaction log backup too old for "<database name>". Risk of disk full in the future: There is a risk that the database transaction log files (LDF files) for this database will expand until the disk is full. The recovery model for this database is set to "FULL" or "BULK_LOGGED" but according to MSDB backup history, the most recent transaction log is too old (older than <minutes> minutes).	Info/Warning

Make script include overview of most recent backups

If you want to view an overview of the most recent backups, for each backup type, for each database, do the following:

1. Delete comment start tag **/*** from the 6th last line.
2. Delete the comment end tag ***/** from the last line.
3. Press F5 or click **Execute** to run the script again.

If you see *NULL* in the **most_recent_backup_finish_date** column, it means that a backup for that database has never been made.

If you see more than one row of information for a single database, it means that multiple types of backups have been made for that database, and each row contains information about the date of the most recent backup of this type.

Defragment indexes in your databases

Databases contain indexes that can get fragmented. Because of that, we recommend that you, on a regular basis, check if you need to defragment your database indexes. If your database indexes have become

too fragmented, see the topic *Maintain Zylinc databases* on Zylinc unified help.

Alternatively, a database administrator (dba) can set up maintenance plans on the SQL server to automatically schedule the tasks mentioned in the previous.

Advanced analysis with SQL Server Profiler

If you are a database administrator (dba), and you want to use SQL Server Profiler to set up a **Trace**, you may find the following **Column Filters** useful:

- **Duration** with the condition **greater than or equal to**, for example, *2000ms* will warn you if queries on your SQL server takes too long to execute.
- **Reads** with the condition **greater than or equal to**, for example, *65000* pages will warn you if queries on your SQL server have become ineffective.

If you identify issues that require changes to, for example, indexes or stored procedures, you need to contact Zylinc support to get assistance to make such changes. This is because the license agreement with Zylinc doesn't permit you to change indexes, stored procedures, etc. in databases provided by Zylinc.

Monitor network port of SQL Server service

We recommend that you monitor the default network port for the SQL Server service, which is typically port 1433/tcp.

Monitor SQL user that Zylinc system uses

The installation guidelines for a typical Zylinc solution describe how to create a new *mixed mode security* user, with the name ZyUser and db_owner database role memberships for the two Zylinc databases, named ZyDB and ZyStatDB.

The Zylinc solution uses ZyUser to access the two databases.

We recommend that you monitor that ZyUser can always access the two databases. Both databases contain a table with the name **database_info** that you can query. This query should always return at least one row.

You can set up two monitoring tasks that uses ZyUser to log in to the two databases ZyDB and ZyStatDB and executes the following query:

```
select * from database_info
```

As mentioned before, the query should return minimum one row.

Monitor that both databases can be updated

Databases can be online and readable, but if the disk that contains the transaction log becomes corrupt or full, or if the database size exceeds the maximum allowed size (which on a SQL Server Express Edition can typically be as little as 10 GB), the database becomes read-only, and the Zylinc solution will no longer work. Again, we don’t want that!

That's why we recommend that you set up two monitoring tasks that check the state of the *updateability* database property for both ZyDB and ZyStatDB

```
SELECT DATABASEPROPERTYEX('zydb', 'Updateability');
```

```
SELECT DATABASEPROPERTYEX('zystatdb', 'Updateability');
```

Each query should return a row that contains the value READ_WRITE.

For more information, refer to the documentation for Microsoft SQL Server and your monitoring tool.

Monitor Zylinc Media Server services

The Zylinc Media Server runs on Debian Linux, and you can use the command line-based management console tool Zylinc AdminCLI to set up its features. You don't have root access to the underlying operating system.

The Media Server provides two important services that you should monitor:

- **Asterisk**: A SIP-based PBX (telephone exchange) service that handles calls to phone queues, and makes it possible for callers to hear music on hold and audio announcements (like “You will be served by the next available representative; please hold …”). Asterisk also makes it possible for callers to use IVR menus (Interactive Voice Response, like “For Sales, press 1”), and many other things like that.
- **Tomcat**: A web server that hosts Administration Portal and provides access to log file downloads as well as upload and download of audio announcement files.

Monitor Asterisk and Tomcat network ports

You should monitor that the two vital services, Asterisk and Tomcat, are running on the Media Server.

Each service should listen on its network port, so you should monitor that those ports respond.

Asterisk ports to monitor:

- Tcp/5038

Tomcat ports to monitor:

- Tcp/8080
- Tcp/8443 (if you use HTTPS)

Monitor Media Server via VMware tools

If you use VMware to host the Media Server, we recommend that you install VMware tools.

VMware tools provide you with advanced monitoring features. To set up monitoring of the Debian Linux server, refer to the guidelines of your organization or to the documentation of VMware and your monitoring tool. You should consider monitoring disk space, memory usage, CPU usage, and the state of time synchronization.

The following steps describe how to install VMware tools on the Media Server:

- Note that Media Server will restart during installation, so you'll need a service window
- Log in to AdminCLI (for example with the tool putty.exe)
- Type `system vmware` to go the VMware section of the shell
- A numbered list of different VMware tools versions is displayed on the screen
- Enter the number of the version of VMware tools to install
- Type `i` to initiate the installation
- Type `y` to confirm that the server will restart

Monitor Media Server via Hyper-V Linux Integration Services

Hyper-V Linux Integration Services is currently not supported on the Media Server. Instead, you can set up monitoring via SNMP, which is described in the following.

Monitor Media Server via installation of a third-party agent

Installation of third-party agents is currently not supported on the Media Server. Instead, you can set up monitoring via SNMP, which is described in the following.

Monitor Media Server via SNMP

You can set up SNMP on the Media Server. This lets your monitoring tool query the server, and retrieve a tree structure of server- and service health-related parameters (OIDs).

The SNMP service will listen to the IP4 address of the Media Server.

The insecure versions 1 and 2c of SNMP will be disabled.

Communication will be encrypted using SHA and AES. The less secure MD5 and DES will be disabled.

The following steps will activate SNMP, so that the command `snmpwalk` and your SNMP based monitoring tool can start to work.

- Log in to AdminCLI (for example with the tool putty.exe).
- Type `feature snmp`
- Type `la`
- Type the IP4 address of the Media Server.
- Type `p` to set a password for authentication protocol pass phrase. The password relates to the -A parameter of the Linux snmpwalk command, or to the -aw: parameter of the Windows snmpwalk command. In this example, we use the password `ppassword`, because you use the `p` command to set it. If you don't change the password, zycallSwitchUser is the default value.
- Type `pr` to change privacy to authpriv.
- Type `at` to change authentication type to SHA
- Type `prs` to change privacy protocol to AES.
- Type `prp` to set a password for privacy protocol pass phrase. The password that relates to the -X parameter of the Linux snmpwalk command or to the -pw: parameter of the Windows snmpwalk command. In this example, we use the password `prppassword`, because you use the `prp` command to set it. If you don't change the password, zycallSwitchUser is the default value.
- Type `v1` to disable version 1/2c.
- Type `v3` to enable version 3.
- Type `t` to enable SNMP service.
- Type `sa` to save.
- Type `w` and you should see the SNMP tree.
- Type `<tab><enter>` to close the SNMP tree.

Use snmpwalk to receive SNMP tree structure

To test that SNMP works, go to another Windows or Linux host and use the snmpwalk command to receive the SNMP tree structure.

Windows:

Download the third party snmpwalk utility from www.snmpsoft.com.

Type this command and replace the user names, passwords and Media Server hostname with the relevant values, as previously described:

```
snmpwalk -v:3 -sn:zycallSwitchUser -aw:ppassword -ap:sha -pp:aes128 -
pw:prppassword -r:MediaServer
```

Linux:

Use any Linux host to get access to the snmpwalk command.

Type this command and replace the user names, passwords and Media Server hostname with the relevant values, as previously described:

```
snmpwalk -v3 -u zycallSwitchUser -A ppassword -a sha -l authPriv -x
aes -X prppassword MediaServer 1.3.6.1
```

Set up SNMP queries in your monitoring tool

From the previous, we now know that SNMP is working as expected, and we even have working command line parameters, that allow us to run an SNMP query from another Windows or Linux host.

We recommend that you set your monitoring tool to use SNMP to monitor disk space, memory usage, and CPU usage on the Media Server.

For information about how to set up alerts and warnings, refer to the guidelines of your organization or to the documentation of your monitoring tool.

An Excel spreadsheet available as an attachment to this document contains a list of all available OIDs on the Media Server. The first column of the sheet is marked with an X for the specific OIDs that we recommend that you monitor as a minimum.

Monitor Windows services

You should monitor some relevant Windows services that run on the Zylinc Windows Application Server.

The names of the services, and the binary paths to the related processes, contain version numbers, so the names and binary paths will change each time you upgrade the system.

That in turn means that if you upgrade the system, you'll also need to review the service names and process names that you've set up for monitoring.

Because of the dynamic nature of service names and binary paths, we don't maintain an exact list of services to monitor. Instead, we'll show you how to quickly extract such a list when you need it:

Extract list of relevant Windows service names to monitor

The names of the services that you should monitor all begin with *zymt_*.

You can use the sc command to extract a list of all services whose names begin with *zymt_*.

On the Zylinc Windows Application Server, open a Windows command prompt.

Copy this line, and run it the prompt:

```
sc queryex type= service state= all|find /i "service_name: zymt_
">1.bat
```

Then run this line in the command prompt:

```
notepad 1.bat
```

A Notepad window will open. You can make the list of services look a little prettier, if you replace all instances of SERVICE_NAME: (note that there should be a space after the colon) with an empty string.

Extract list of binary file paths to monitor

Do the following to extract a list of the binary paths of all the services whose names begin with *zymt_*.

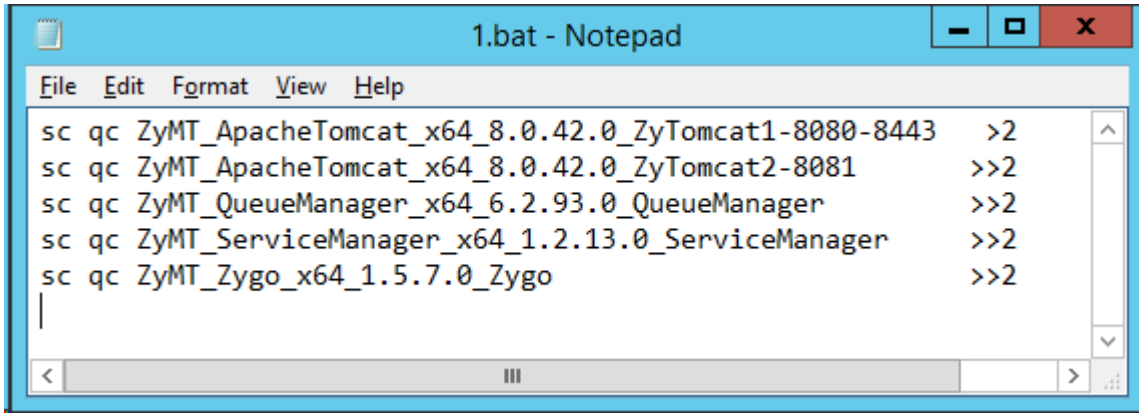
Open a Windows command prompt, and run these two lines one after the other in the command prompt:

```
sc queryex type= service state= all|find /i "service_name: zymt_
">1.bat
```

```
notepad 1.bat
```

A Notepad window will open:

- Replace all instances of SERVICE_NAME: (again with a space after the colon) with sc qc (with a space after sc qc).
- Add `>2` to the end of the first line
- Add `>>2` to the end of all the other lines, like in this example:



- Save, and then exit Notepad.

Now, run these three lines one after the other in the command prompt:

```
1.bat
```

```
find /i "binary_path_name" <2>3.txt
```

```
notepad 3.txt
```

A Notepad window will open, and you'll see a list of the binary paths for all the service processes.

Excel spreadsheet: Ports to monitor on Windows

To give you a good overview of the many different Zylinc services and modules, we have an Excel spreadsheet that you can use to decide which network ports you need to monitor on your Zylinc Windows Application Server.

The spreadsheet contains all known network ports of the system.

You can download the spreadsheet from Zylinc unified help.

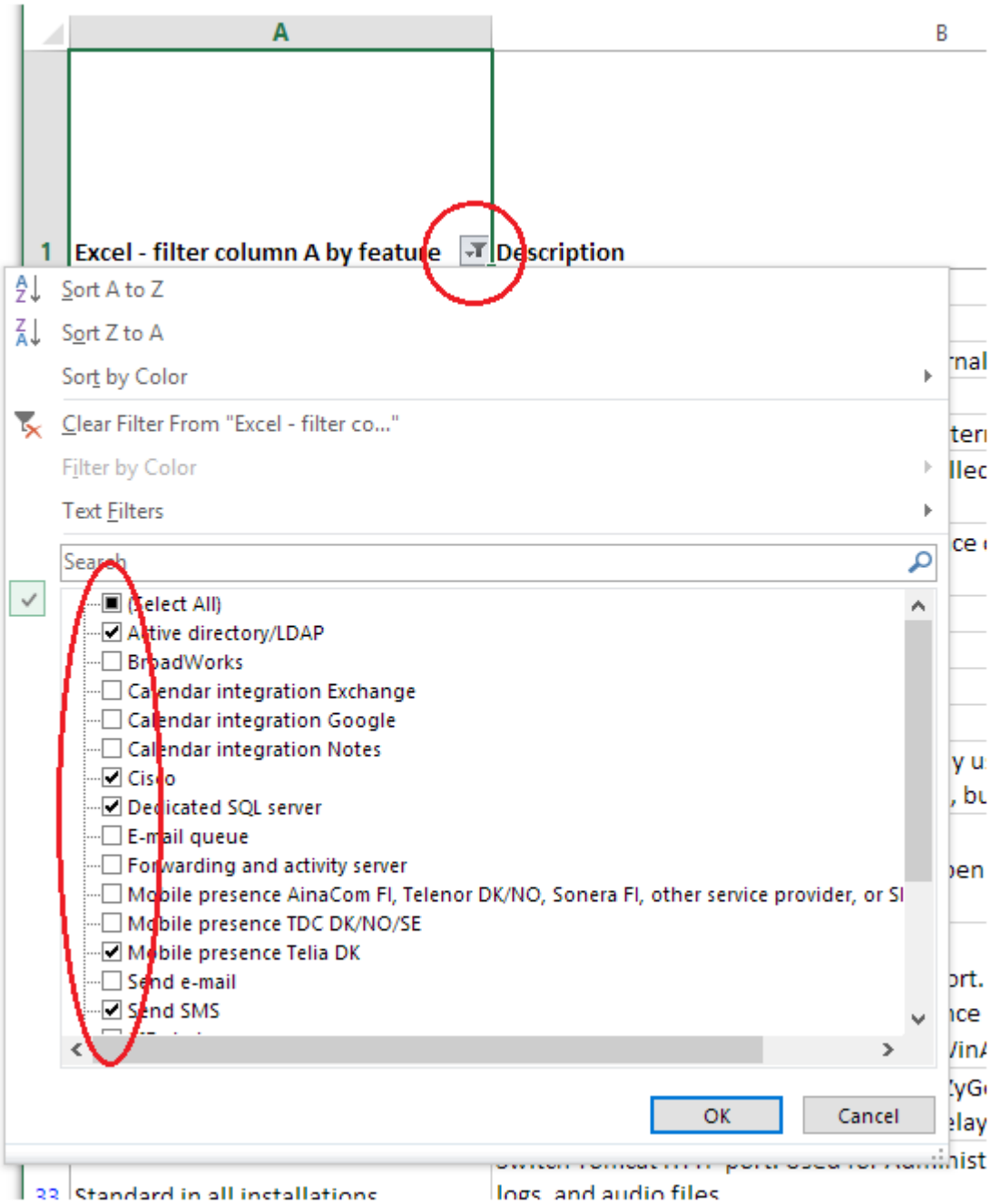
You can use a filter on column A to select **Standard in all installations** in addition to any add-on features that you use.

Add a filter on column J, **We recommend that you monitor this port if you use the feature**.

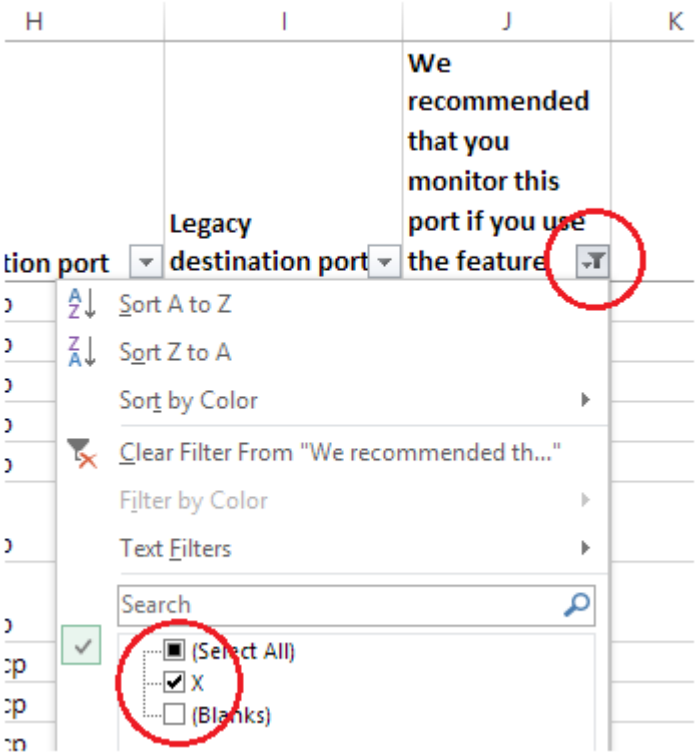
Add a filter on column G, **Destination host**, to select ports for Windows application server.

The following steps describe how to do that:

- Click the filter button in the bottom right corner of cell A1.



- Select **Standard in all installations** as well as any additional features that you use.
- You can now add an additional filter that will select only the ports that we recommend that you monitor. Click the filter button in the bottom right corner of cell J1 and select the filter with the name **X**:



- Add a similar filter to column G (**Destination Host**) that selects the rows marked with **WinAppServer**. This will show you all the ports to monitor on Windows application server (WinAppServer).

You'll now have a filtered list that shows you:

- The network ports that are standard in all installations, plus the additional features that you use
- Only the network ports that we recommend that you monitor
- Only the network ports on Windows application server

Monitor Tomcat services on Windows

Tomcat is a Java-based web server. Several of the software modules in a Zylinc solution use Tomcat, so those modules require Java and an instance of Tomcat to be able to run.

You can use the Zylinc Deployment Manager (that comes with the Zylinc solution) to *create* as many instances of Tomcat services as you need. Typically, you'll have two instances.

Each instance can use arbitrary versions of Tomcat as well as Java. Several instances can co-exist, as long as you use distinct names and distinct network ports. You can also use Deployment Manager to *install* any of our Tomcat-based software modules on any of the Tomcat instances that you've created.

Monitor network ports of Tomcat instances

You should monitor some network ports that the Zylinc solution's Tomcat instances use.

Generally, each Tomcat instance listens on three or four ports, depending on whether you've enabled support for HTTPS or not.

If you use the port numbers that the installation guide for a typical Zylinc solution recommends, you'll want to monitor the following ports:

Tomcat instance 1 ports to monitor

- Tcp/8005 (*localhost only*)
- Tcp/8009
- Tcp/8080
- Tcp/8443

Tomcat instance 2 ports to monitor

- Tcp/8006 (*localhost only*)
- Tcp/8010
- Tcp/8081

If you run the port monitoring agent from another host on the network, you can't monitor the ports marked with (*localhost only*). In that case, you won't be able to monitor ports 8005 and 8006.

Monitor services and processes of Tomcat instances

When you create Tomcat instances in Deployment Manager, a Windows service is created for each instance. The Tomcat Windows services will be given the name *ZyMT_ApacheTomcat_x64_<version>_* followed by the name that you've entered for the instance.

For all Tomcat instances that you use, you should monitor that those Windows services are running.

If you use the instance names that we recommend in the installation guide for a typical Zylinc solution, you'll want to monitor the services that have the following names:

Tomcat instance 1 service name

- ZyMT_ApacheTomcat_x64_8.0.42.0_ZyTomcat1-8080-8443

Tomcat instance 2 service name

- ZyMT_ApacheTomcat_x64_8.0.42.0_ZyTomcat2-8081

> ⚠ Note that version number 8.0.42.0 is an example. The version number may be different on your installation.

Tomcat process names

The process name for all Tomcat instances is *tomcat8.exe*. To identify a process that belongs to a specific instance, you can use the PID for the running service and compare it to the PID of the tomcat8.exe processes.

Monitor specific network ports of Tomcat modules

You can monitor that some of our Tomcat-based software modules listen on their configured network ports. If more than one port exists, both ports should respond.

The following Tomcat modules use a specific network port that you should monitor, if you use the modules in your organization:

Client Manager

- Tcp/35033
- Tcp/35034

Messaging Portal

- Tcp/35028 (optional module)

Zylinc Proxy

- Tcp/35031 (optional module)

Zylinc Proxy Client

- Tcp/35032 (optional module)

The rest of the Tomcat modules don't listen to a specific port. You can use active checks, as described in the following, to monitor them.

Monitor all Tomcat modules via active checks

Active checks is a feature that's useful when you need to monitor that a web service located at a specific URL is responsive. The feature works in a way similar to the well-known wget command, and is available in many third-party monitoring tools, for example under the name *check_http*.

You can use active checks to validate that all your individual Tomcat modules are reachable and responsive.

If you use the instance names that we recommend in the installation guide for a typical Zylinc solution, the following table contains the information that you need to set up active checks in order to monitor all the Tomcat modules.

You should monitor all the modules that are marked as mandatory. Optional modules must be monitored if they're installed on your system.

The base URL for each tomcat instance is http://<server>:<port>/

Tomcat module name	Server	Port	URL to get	Expected result	Mandatory
Admin Portal (zylinc-admin)	Media	8080	/zylinc-admin	200 OK	×
Authentication Server	App	8080	/Authentication	200 OK	×
ClientManager	App	8080	/ClientManager	200 OK	×
Stat Portal	App	8081	/StatisticsPortal	200 OK	×
ZyCore ID	App	8080	/ZyCoreID	401 Unauthorized	×
ZyDataService	App	8081	/ZyDataService	200 OK	×
Cisco Directory Sync.	App	8080	/CiscoDirSync	401 Unauthorized	
Cisco User Proxy	App	8080	/CiscoUserProxy	401 Unauthorized	
Lync Web Chat	App	8080	/LyncWebChat	200 OK	
Messaging Portal	App	8080	/MessagingPortal	200 OK	
Sametime Presence v2	App	8080	/SametimePresence	401 Unauthorized	
Zylinc Proxy	App	8080	/ZylincProxy	200 OK	
Zylinc Proxy Client	App	8080	/ZylincProxyClient	200 OK	
Zyte	App	8080	/Zyte	200 OK	

Some examples of complete URLs to check:

- http://<windows application server>:8080/ClientManager/
- http://<windows application server>:8081/StatisticsPortal/
- http://<MediaServer>:8080/zylinc-admin/

Get alerts if queues become too busy, etc.

If you have administrator rights on the Zylinc solution, you can set up queue alarms. With queue alarms, your Zylinc solution can automatically send out alert messages when a queue becomes too busy, when too few agents monitor the queue, or similar.

The Zylinc solution can send queue alarms as either e-mails, text messages (SMS), or both.

If the system already knows the e-mail addresses or mobile phone numbers for the agents on a queue (which should normally be the case), you can select to send the queue alarms to one or more of the agent groups *primary*, *secondary*, or *standby* (the latter is a special group of agents who are meant to help out on busy queues). This option is simple to use, because you don't need to enter e-mail addresses or mobile phone numbers for agents who are already known to the queue. It's useful if you have agents who may have forgotten to log in, or have failed to answer an inquiry, and therefore have become unavailable on the Zylinc system.

If the system doesn't know the e-mail addresses or mobile phone numbers of the agents on a queue, or if you want to send queue alarms to addresses or phones outside of the standard groups of agents, you can specify a list of additional addresses or phone numbers to send queue alarms to. This is useful if you yourself, a call center manager, a general manager, or some other manager or supervisor (but not an agent) wants to receive queue alarms.

You can of course set up thresholds and trigger timers, so that you don't get spammed with unnecessary queue alarms.

Queue alarm events

Queue alarms works for voice queues, e-mail queues, and chat queues, and you can set up alarms for the following events:

- **Unmonitored:** Sent when an open voice queue, chat queue, or e-mail queue, hasn't been monitored by any agents for the specified amount of time (in seconds).
- **Max waiting time:** Sent when an inquiry has been waiting in an open voice queue, chat queue, or e-mail queue for at least the specified amount of time (in seconds).
- **Max number of calls:** Sent when at least a certain number of inquiries are waiting in an open voice queue, chat queue, or e-mail queue.
- **Min number of agents:** Sent when less than a certain number of agents monitor an open voice queue, chat queue, or e-mail queue.

Timers prevent unwanted queue alarms

To prevent repeating or unnecessary alarms, you can set up a trigger timer and an alert sanity timer.

Trigger Timer (unmonitored) makes the solution wait for a certain amount of time before the *unmonitored* type of queue alarm is sent. This way you can avoid false alarms, for example if a user logs out and then logs in again shortly after when a computer restarts, or when a user changes client type from ZyDesk (on a computer), to Mobile Agent.

Alert Sanity Timer makes the solution wait for a minimum time after one alert has been sent, before the next can be sent. This way you can avoidt duplicate alarms.

Example: E-mail alert via Office 365 when queue is unmonitored

Task 1: Set up Messaging Portal and SMTP account

1. In the Administration Portal menu, select **INSTALL > Portal Configuration**
2. Select **Messaging**, and click **Save**
3. In the Administration Portal menu, select **SYSTEM > Mail Accounts**
4. Click **Add Mail Account**
5. In **Name**, enter a name for the mail account, for example `Office 365`
6. In **SMTP Settings**
   a. In **SMTP Server**, enter `smtp.office365.com`
   b. In **Port**, enter `587`
   c. Select **SSL**
   d. In **User (default)**, enter the e-mail address and password for the user account that you want to send e-mails from. Make sure the SMTP account you use, can send on behalf of the agents.
   e. Click **Save**
7. In the Administration Portal menu, select **NETWORK > Messaging Gateway**
8. In **Gateway URL**, enter an URL similar to `http://<win-appserver>:35028/MessagingPortal`

Task 2: Deploy Tomcat service Messaging Portal to primary Tomcat instance

1. In the Deployment Manager menu, select **Deployment > Tomcat Services**
2. In **Instance**, select the instance on port 8080 that already hosts *Authentication*, *Client Manager*, and *ZyCore ID*
3. In **Available Tomcat applications**, select **Messaging Portal**, and click **Deploy Services**

Task 3: Send test e-mail message from Messaging Portal

1. In a web browser, open an URL similar to `http://<win-appserver>:8080/MessagingPortal`, and log in as `admin` with the password for Tomcat instance ZyTomcat1-8080-8443 user `admin`
2. In the Messaging Portal menu, select **TEST EMAIL**
3. In the **To Email** and **From** fields, enter the e-mail address of the user account that you want to send e-mails from

   Just use the same address in both fields.

4. Click **Test email**

You should see a status message similar to the following:

```
Test Result:
Response Http Status Code: 200
```

```
Result: Email sent successfully
Error Message: No error message
Gateway Response Result: Email sent successfully
```

If you see an error, you can view information about the error directly on the screen, or you can open the log file for the Tomcat service **Messaging Portal** and inspect the bottom of the log file for information about the error. To locate the log file, see Open latest log file from specific Zylinc module

Typical errors are caused by wrong SMTP hostname, SMTP port, user name, or password, or a firewall rule that blocks outgoing connections to the specified SMTP server.

Solve any errors and make sure that the Messaging Portal can send e-mails before you continue to the next step.

Task 4: Set up queue alarm

1. In the Administration Portal menu, select **INSTALL > Portal Configuration**
2. Select **Queue Alarms**, and click **Save**
3. In the Administration Portal menu, select **QUEUES > Queue Alarms**
4. Click **Add Queue Alarm Configuration**
5. In **Queue to monitor**, select the queue for your queue alarm
6. In **Unmonitored**, select **Send mail**
7. In **Unmonitored, Mail subject**, enter `Queue Alarm: unmonitored queue <name of your queue>`
8. In **Unmonitored, Mail text**, enter `Queue Alarm: No agents are currently monitoring the queue <name of your queue>`
9. In **Settings, Mail sender**, enter the e-mail address of the account you use to send the e-mail from
10. In **Settings, Additional mail receivers**, enter the address of the person who should get the e-mail alert.

Task 5: Test that queue alarm works

1. Log in to ZyDesk as an agent who subscribes to the queue that has the queue alarm
2. Call the queue, and click **Answer**
3. Click **Hang Up**
4. Close ZyDesk

An e-mail that contains the queue alarm should arrive in the inbox of the e-mail address that you specified in **Additional mail receivers** for the queue alarm.

How to solve errors related to queue alarms

Queue alarms are handled by a Tomcat Service with the name **ZyDataServices**, together with a Tomcat

service with the name **Messaging Portal**

1. Open the log files for those two modules and inspect the log files for errors that relate to queue alarms. See Open latest log file from specific Zylinc module
2. In the log file for **ZyDataServices**, it's a good idea to search for the word *AlarmHandler*, and the words *Error* or *Exception*. In the log file for **Messaging Portal**, there should be a complete log of all the SMTP activity. This log file can be useful to find the source of errors.

Copyright, trademarks, and disclaimer

Third-party hardware & software – impact on Zylinc support

Zylinc solutions integrate with numerous third-party hardware and software providers. Some of the third-party software is essential to the core operation, for example operating systems and databases. Other third-party software is needed to implement additional features, for example chat. Third-party hardware, like phones or headsets, can also play a great role in a Zylinc solution.

To guarantee a fully working solution, Zylinc closely follows the release cycles of the third-party hardware and software vendors. Zylinc will not support integration to third-party hardware or software that's no longer supported by the respective vendor. This also applies to hardware and software that isn't directly used in the Zylinc solution as such, but can be used as tools that support the general use of the Zylinc solution, for example Microsoft Excel.

- **Microsoft**
  Zylinc solutions aren't supported on Microsoft software that has passed its Mainstream Support end date. Zylinc doesn't support Microsoft products in the Extended Support state.
  You can find the official Microsoft lifecycle definitions at https://support.microsoft.com/en-us/gp/lifeselect, from where you can also find detailed lifecycle information on specific products.
- **Cisco**
  You can find infomation about the lifecycle of Cisco Call Manager at https://www.cisco.com/c/en/us/products/unified-communications/unified-communications-manager-call-manager/eos-eol-notice-listing.html
- **Third-party APIs in general**
  Many third-party software and service providers don't follow strict software lifecycle policies where changes to APIs are announced well in advance. This applies to, for example, Facebook and Google. Zylinc follows updates to all relevant APIs closely, and will update the Zylinc solutions to comply with updates as quickly as possible. However, Zylinc isn't responsible for any limitations, thresholds, etc. in such third-party APIs.
- **Third-party hardware**

Many third-party hardware providers don't follow strict lifecycle policies where changes to their hardware and any associated software, firmware, etc. are announced well in advance. This applies to, for example, phone device and headset manufacturers.
Zylinc follows updates to all relevant hardware as closely as possible, and will update the Zylinc solutions to comply with updates as quickly as possible. However, Zylinc isn't responsible for any limitations, etc. in such third-party hardware.

When you upgrade or downgrade third-party software or hardware that could have an impact on how your Zylinc solution will work, we strongly recommend that you test the upgrade or downgrade in an isolated test environment before you apply the changes in your production environment. You should be especially aware of this if you subscribe to automatic third-party updates.

If you're in doubt about whether particular third-party software or hardware will work with your Zylinc solution, you're welcome to contact Zylinc support for advice.

No warranties

Unless you are provided with a specific warranty from Zylinc as part of your product documentation, Zylinc expressly disclaims any warranty for the product.

The product and any related documentation is provided “as is” without warranty of any kind, either expressed or implied, including, without limitation, the implied warranties of merchantability or fitness for a particular purpose. The entire risk arising out of use or performance of the product remains with you as the user.

Limitation of liability

In no event shall Zylinc or its suppliers be liable for any special, incidental, indirect, or consequential damages whatsoever (including, without limitation, damages for loss of business profits, business interruption, loss of business information, or any other pecuniary loss) nor for any product liability (except for bodily injury) arising out of the use of or inability to use the product or the provision of or failure to provide proper support, even if Zylinc has been advised of the possibility of such damages.

Absent any willful misconduct or gross negligence, the entire liability of Zylinc and its suppliers shall be limited to the amount actually paid by you for the product.

Enterprise orders

When Zylinc partners deal with orders that involve Zylinc, they can greatly benefit from using the recommended standard delivery process (available on Zylinc unified help). However, when Zylinc partners deal with enterprise orders, that is orders that involve Zylinc solutions for more than 500 end users, they *must* use the standard delivery process.