Workflow Templates Library

Table of Contents

Intro

Ayehu eyeShare includes a list of built-in workflow templates which are used to solve common organizational issues. The templates are divided into different IT categories and are described in the following sections. In order to use the templates, drag and drop the requested template from the Workflow Template pane and into the Sequential Workflow pane.

Active Directory

Template	The Process…
AD User Synchronization	Synchronize users, groups and OUs from Active Directory to eyeShare.
Add user to AD group upon incoming email	Creates new account in the AD, according to information that was received by incoming email. The email includes the user name and required AD group.
Add users to group according to Excel file	Uses an Excel file to add users to a group. Using this process, you can add the users to a specific group, or alter it to get the group name as a variable.
Create disabled users report	Creates report about disabled users in the AD. The workflow can be scheduled on a regular basis.
Create locked users report	Creates report about locked users in the AD. The workflow can be scheduled on a regular basis.
Create new user accounts from a pre-defined list	Uses an Excel file to create new AD users. The Excel file contains the user name, its first name, last name and an email address. You can add more details to it as you wish (e.g. cell phone number or employee ID). You can also use the Generate Password activity to create a different password for each user and send it to the user via SMS after creation. The Excel file can be generated from your HR system and be easily used by eyeShare in this simple process.
Create password never expires report	Creates a report of users that their password is set to "never expires" and emails the report to Admin.
Create users' passwords expiration report (Admin)	Checks how many days are left for every user in a specific OU, and sends a report to the administrator. This process can help to avoid unnecessary calls to the help-desk team, and can also be combined with another automatic process that resets the user's password it is expired or forgotten.
Delete disabled users	Retrieves the list of all users in a specific OU and deletes the disabled users. At the end of the process the deleted user report is sent to Admin user.

Template	The Process…
Enable/Disable list of users	Enables / Disables list of AD users on pre-defined time frames.
Find AD zombie computers	Provides an easy and efficient way to create a report of computers that did not log in to the domain within a specific time frame. Using this template you can maintain your AD on a regular basis while keeping it organized and updated.
Find AD zombie users	Provides an easy and efficient way to create a report of users that did not log in to the domain within a specific time frame. Using this template you can maintain your AD on a regular basis while keeping it organized and updated.
Password expiration notification	Checks how many days are left for every user in a specific OU, and sends an email to the users if necessary. This process can help to avoid unnecessary calls to the help-desk team, and can also be combined with another automatic process that resets the user's password it is expired or forgotten.
Reset user password by sending text message to eyeShare	Resets a user's password and sends the new password via SMS. You can also alter this process to generate a random password instead of a pre-defined one.
Set AD user property	Sets AD user property. The property type and value can be dynamic.
Unlock locked users	Verifies all users in a specific OU are locked, and sends an email to unlocked users.
Users termination procedure	Uses an Excel file or a memory table to delete obsolete users from the AD and handle other activities that are related to a work termination process, such as compressing and backing up the user profile. The Excel file can be generated from your HR system and be easily used by eyeShare in this simple process to help maintain your AD free from former employees' users and keep your company safe.

Application

Template	Description
Check if antivirus process is running	Checks that a specific process is running (you should provide the name of your anti-virus process) on a device. You can alter this process to retrieve a list of devices from an Excel file or a memory table and check if the process is running on all of them. Use this process to protect your company's devices from malware and other risks.
Check if backup process is over	Retrieves a list of servers from an Excel file or a memory table and checks for the amount of backup processes running on each server. According to the process amount running on the server a variable is updated with the server's name and its backup status. At the end a report is sent to the administrator.
Check if service is running	Checks if a specific service is running on a server, and if it is not, communicates a focal point of your choice and asks if the service should be started. In case the answer is "Yes", the service is started. You can schedule this process to run daily / hourly or use it as a part of another workflow handling an incident.
Create anti-virus inventory report	Retrieves a list of servers from an Excel file or a memory table and checks if Anti-Virus software is installed on each server on the list. Each time the software is found installed on a server, the server's name is added to a list held in a memory table, and at the end of the process this list is sent to the relevant personnel. This process can be scheduled to run daily, and will help you verify all your servers are protected with the latest version of Anti-Virus.
Create software inventory report	Retrieves a list of servers from an Excel file and checks if specific software is installed on each server. Each time the software is found installed on a server, the server's name is added to a list held in a variable, and at the end of the process this list is sent to the relevant personnel. This process can be scheduled to run daily and will help you keep an updated inventory of software installations in your company.
Find top 5 CPU consuming processes	Retrieves a list of the top 5 CPU consuming processes, and emails the report in an HTML format.

Template	Description
Find top 5 memory consuming processes	Retrieves a list of the top 5 memory consuming processes, and emails the report in an HTML format.
Find unauthorized installed software	Retrieves a list of servers from an Excel file and checks if specific software is installed on each server. Each time the software is found installed on a server, the server's name is added to a list held in a variable, and at the end of the process this list is sent to the relevant personnel. This process can be scheduled to run daily and will help you keep you company clean from unauthorized software.
Kill a stuck process	Retrieves the information of a specific service, and calculates the memory usage in a 1 minute interval. If the calculated data is equal to the retrieved data, the process is assumed to be stuck and killed.
Monitor services on a list of servers	Retrieves a list of servers from an Excel file or a memory table, which contains a combination of Servers and their Services, and verifies that each service is running on its designated server. At the end of the process a report of all stopped services is sent to the administrator.
Set service credentials	Sets a service logon credentials on a list of servers.
Stop and disable service	Stops and disables a service on a list of servers.

Cisco Tasks

Template	Description
Backup Cisco configuration	Backs up the configuration of a list of cisco routers in files.
Create Cisco routers version report	Creates a version report of a list of cisco routers.
Display IP routing table	Displays the router's IP routing table.
Overview all interfaces on the router	Creates a report of all IP interfaces in a router.
Show router interface status	Displays the router's log.
Show router logs	Checks for the status of a specific router's interface.

Database

Template	Description
Check for errors in a database table	Retrieves all data from a specific table, and searches for the phrase "Error". If the phrase exists, a table of all rows containing the word "Error" is emailed to the focal point.
Check number of rows in database table	Retrieves all data from a specific table, checks for the number of rows in the table and sends an email in case the number of rows exceeds a pre-defined threshold.
Compare two database tables	Compares the contents of two database tables and sends the difference report to the Admin user.
Send SQL query result via HTML	Retrieves all data from a specific table, converts it to HTML and sends the result by email.

Excel Automation

Template	Description
Compare Excel files contents	Compares an original Excel file with a list of Excel files in a list of servers (all files should have the same structure) and sends a report if there are any differences.
Delete specific rows from Excel file	Deletes specific rows (according to a contained value) from an Excel file, and sends the new updated file to the Admin user.
Migrate database table into Excel file	Reads information from a DB table using query activity, and writes the data to an Excel table.
Migrate Excel file into database table	Migrates an Excel file into an SQL table by adding rows to the DB table using a T-SQL statement.
Read Excel file and send result in HTML format	Converts an Excel file to an HTML table and sends it by email.
Return number of columns in Excel file	Checks the number of columns in an Excel file and sends it by email.
Return number of rows in Excel file	Checks the number of rows in an Excel file and sends it by email.

Files and Folders

Template	Description
Archive files older than 30 days and delete original	Retrieves a list of all files, in a specified location, which are older than 30 days. The process compresses these files to a zip format, copies the zipped file to a remote server, and deletes the original file. Use this process to keep free space on your production servers, and archive old logs on a destination backup server.
Backup and zip folder	Backs up and compress specific folder.
Backup files	Backs up a file on a group of servers by copying it to a target destination and adding the time and date data to the file name.
Checks file modification date and time	Checks file modification date and time, and send alert in case it was not changed within certain time period.
Check if file exists	Checks for a specific file in a specific folder. If the file does not exist, an email is sent to the Admin user to request file creation approval.
Compare DLL versions	Checks if the versions of two files are identical on a list of servers, and sends a report. It can be useful to issue a report of all servers with DLL files which are not updated.
Compare folder's contents	Compares the files in two folders and copies all files that do not match to a third folder for examination.
Compare two configuration files	Checks if two configuration files are identical or different on a list of servers and sends a report to the Admin user. Use this process to assure all configuration files in your organization have not been touched by unauthorized personnel.
Compress files larger than 5 MB	Retrieves a list of all files in a specific folder on a group of servers, and creates a ZIP file from any file that is larger than 5 MB. This process can be followed by a Delete File activity (to delete the original file) to help you maintain your servers' free disk space.
Delete all empty files	Retrieves a list of all files in a given directory, and deletes every file of 0 KB.

Template	Description
Delete all empty folders	Retrieves a list of all folders in a given directory, and deletes every folder of 0 KB. This process will help you maintain your server cleaner and easier to navigate in.
Delete all MP3 files	Retrieves a list of all MP3 files in a given directory, and deletes them.
Delete duplicate rows from a file	Reads the contents of a file, and, using the "select distinct" statement, returns the distinct rows and writes them back to the file.
Delete files older than 30 days	Deletes every file in a specific folder on a group of servers that is older than 30 days. It can either be used as a scheduled process to maintain your servers' free disk space, or as part of a disk clean up policy in case of an incident.
Delete largest 5 files upon request	Retrieves a list of the largest 5 files in a folder, and requests approval for deletion. The approver can select which files to delete.
Download file and distribute it	Downloads file from the provided URL and distributes it between list of servers.
Find the largest file in the folder	Retrieves a list of all files in a specific folder, sorts them by s descending file size and returns the first file on the list.
Find the newest file in the folder	Retrieves a list of all files in a specific folder, sorts them by a descending creation date and returns the first file on the list.
Merge two text files	Combines two text files (one after the other) and stores the combination in a new file.
Monitor file access date	Monitors file last access date and sends report in case it is higher than certain time period.
Monitor log files	Searches for specific keywords in a log file on a group of servers, and, if found, sends the relevant rows as an HTML report by email. The process can be scheduled to run in specific intervals, thus providing a reliable and easy to configure monitor of the log file. Note that every time the process runs it starts reading the log from the last row that was previously examined.
Read specific line from a text file	Reads a specific line (by name or number) from a file and sends it by mail.

Template	Description
Replace specific characters in a text file	Searches for a given string in a text file and replaces it with another string.
Return number of lines in a text file	Counts the number of lines in a specific file and sends the results by email. This process can be used to track down log files which hold any information besides the title/time, or log files that have grown since the last check.

FTP Tasks

Template	Description
Delete 0KB files from the FTP server	Opens an FTP connection and retrieves a list of all existing files in a given path. Then checks the size of each file and if it is 0 KB the file is deleted.
Delete files older than 30 days from FTP server	Opens an FTP connection and retrieves a list of all existing files in a given path. Then checks for each file's create date. If the file was created before the last30 days it is deleted. Use this process to delete obsolete files and keep free space on your FTP server.
Delete large files from the FTP server	Opens an FTP connection, and retrieves a list of all existing files in a given path. Then checks the size of each file and if any of them exceeds the defined limit the file is deleted.
Download and delete the largest file	Opens an FTP connection and retrieves a list of all files in a given path, sorts them by their size (descending) and deletes the first file in the list. Use this process to keep free space on your FTP server.
Download and Monitor FTP file download	Monitors the progress of a file download from the FTP servers, by comparing its current size with its size 30 seconds before the check, until they are identical, and sends an alert when the download is completed. You can schedule this process to run daily in a specific time of the day if you are expecting a file's download to complete within a fixed time frame.
File Management Automation	Downloads a zip file from an FTP server, and checks that the file was not corrupted by decompressing the file and searching for a specific phrase inside the file.
Rename a file on FTP server	Opens an FTP connection and adds the current date and time to the file name. You can use this process to keep old file versions on your server.

Incident Management

Template	Description
Change Management Procedure	Requests for approval to perform an activity from two different managers. Only if both approved, the approval is sent. Otherwise everyone is notified which manager did not approve the performance. This procedure should be initiated as a result of an external email alert, in which the subject holds the request's information.
Incident management procedure	Escalates an incident and waits for a response from someone in the escalation list. In case no one responds, an email is sent to inform no one is handling the problem. In case of a response the workflow follows up (every minute) with the person who took ownership, and closes the incident when it is reported as solved.
Increase incident severity every 10 minutes	Checks incident status every 10 minutes and increase its severity in case it is not closed.
Monitor incidents that have been opened for over 30 minutes	Monitors open incidents and sends alerts regarding incidents which are open more than 30 minutes.
Monitor critical incidents	Monitors all open incidents and sends alerts regarding the critical alerts which are currently open.
Open incidents report	Retrieves a list of al open incidents in the system and sends it by email.
Response action menu	Escalates an incident, waits for one of the responses (CPU, Memory or Disk), and continues the activities according to the reply. You can use this process as a part of another workflow when handling an incident.
Send email to a list of email addresses	Retrieves a list of email addresses from an Excel file or a memory table and sends an email to each address.
Send text message to a list of recipients	Retrieves a list of cell phone numbers from an Excel file or a memory table and sends a text message to each address.

Security & Compliance

Template	Description
Alert when admin account created	Searches for a specific event code in the Security Event log, and, if exists, sends the relevant records in the form of an HTML table by email. Schedule this process to run on an hourly basis to keep track of security breaches in your organization.
Audit changes to security policies	Searches for a specific event code in the Security Event log, and, if exists, sends the relevant records in the form of an HTML table by email. Schedule this process to run on an hourly basis to keep track of security breaches in your organization.
Audit failed logon attempts	Searches for a specific event code in the Security Event log, and, if exists, sends the relevant records in the form of an HTML table by email. Schedule this process to run on an hourly basis to keep track of security breaches in your organization.
Disable root login Linux	Disables root login on list of Linux servers.
Find services which are running with admin user	Monitors services on list of servers and sends alert regarding services which are running with admin user.
Monitor if user was added to a local security group	Monitors security event log on list of server, in order to find if users were added to local security group.
Monitor Security event Log	Monitors the Security event log, and searches for the phrase "Failure". Run this process on an hourly basis to keep track of your system problems.
Start Anti-Virus Service	Starts the Anti-Virus service on a list of servers.
Start Windows firewall	Starts Windows firewall on list of servers.

System Tasks

Template	Description
Automate Linux command	Executes any required command on list of Linux servers.
Create OS inventory report	Create report that includes server name and the OS which is installed on this server.
Create servers' status report	Reads list of servers and creates a report about each server which includes server status, CPU usage, memory usage, disk space usage and service status.
Free up disk space	Retrieves a list of servers from an Excel file or a memory table which contains the server names. According to the list, checks every server's current disk space. In case it exceeds the desired threshold a pre-defined file is deleted and an email is sent. You can also add a "focal point" column for each server and use this process to quickly and easily notify the relevant person whenever a problem occurs, and add more file deletion activities to maintain your servers' free space.
Monitor backup log	Reads the content of a backup log file, each time starting from the end of the previous file reading. The process searches for the phrase "Backup Failed" within the newly written lines. Matching lines are sent by an HTML report to the backup focal point.
Monitor disk space	Retrieves a list of servers from an Excel file or a memory table which contains the server name, disk name to monitor, and the threshold for each disk. For each disk, the process checks if the current disk space exceeds the desired threshold, and if it is an email is sent. You can also add a "focal point" column for each server and use this process to quickly and easily notify the relevant person whenever a problem occurs.
Monitor mail service using an external address	Sends a mail to an external mail address and waits for an automatic response for a pre-defined time frame. If there is no response the Admin user is alerted with an SMS and an IM. This process can be scheduled to run hourly to make sure your service is available.

Template	Description
Monitor servers' availability	Retrieves a list of servers from an Excel file or a memory table and checks if the server is up or down. In case the server is down, an email is sent to the focal point. You can also add a "focal point" column for each server and use this process to quickly and easily notify the relevant person whenever a server is down.
Monitor servers' uptime	Retrieves a list of servers from an Excel file or a memory table which contains server names, and for each server checks the current uptime. If the uptime exceeds a pre-defined threshold, the server name is added to an HTML report and sent to the relevant personnel.
Monitor System event log	Monitors the System event log, and searches for the phrase "Error". Run this process on an hourly basis to keep track of your system problems.
Servers log off procedure	Retrieves a list of servers from an Excel file or a memory table and checks if the server is up or down. In case the server is up a log off process is performed, and at the end of the process a report is sent to the Admin user. Use this process to protect your company's computers and network from being abused by unauthorized personnel.
Servers Restart procedure	Retrieves a list of servers from an Excel file or a memory table and checks if the server is up or down, and at the end of the process a report is being sent to the Admin. In case the server is up a restart process is performed. Use this process to maintain a weekly / monthly restart procedure to maintain the servers' health.
Servers shutdown procedure	Retrieves a list of servers from an Excel file or a memory table and checks if the server is up or down. In case the server is up a shutdown process is performed, and at the end of the process a report is sent to the Admin user. This process can be used for two main purposes: to shut down your servers quickly in case of an emergency (when moving to a DRP site or when the Data Center is not in ideal environmental state). The second is to shut down all PCs in the company on a specific time every evening or when the weekend starts, to save in resources and become a more "green" company.
Switch to DRP	Turns off a list of servers and starts another list of servers in a reverse order.

Template	Description
Wake on LAN procedure	Retrieves a list of physical servers from an Excel file or a memory table and starts every server. At the end of the process a report is sent to the Admin user containing all servers that were not started.
Switch to standby	Retrieves a list of workstations from an Excel file or a memory table and checks if a screen saver process is running on them (to check if someone is working at the moment). In case there is a screensaver running, a switch to stand-by process is performed.
Workstation hibernate procedure	Retrieves a list of workstations from an Excel file or a memory table and checks if the workstation is up or down. In case the workstation is up a hibernation process is performed.

VMware Tasks

Template	Description
Create a list of power off machines	This template reads a list of virtual machines, and checks the state of each machine. In case the power state is off, it will the machine name to the final report.
Create snapshot on a list of virtual machines	This template reads a list of servers from an Excel file, and creates a snapshot for each VM. It might be very useful before maintenance procedure if a mass software installation.
Create snapshots report	This template creates a snapshots report for each virtual machine. The report contains the machine name, snapshot name and creation date. The report is being saved to excel file and can be sent to the system administrator as well.
Create VM capacity report	This template creates a report about the number of hosts and VMs on the virtual center. It goes over the list of hosts, and finds the VM list on each host, while adding it to the final report.
Create VMs inventory report	This template creates a report of each VM including its information.
Delete old snapshots	This template retrieves a list of virtual machines, while deleting snapshots older than 30 days on each machine. It can be used in order to maintain your virtual environment on a regular basis.
Delete specific snapshot on a list of virtual machines	This template read a list of servers from an Excel file, and deletes a specific snapshot on each machine. This workflow can be used for example, to delete a snapshot that was taken before an upgrade across your virtual environment.
Deploying Virtual Machine from Template	This template reads an Excel file which includes the required parameters from the new virtual machine. It uses the VM clone activity in order to create the machine according to the requested parameters.
Power on list of virtual machines	This template reads a list of servers from an Excel file and power on each server. When the procedure is done, it waits 5 minutes and confirms that all servers are up. In case that few of them are still down, it will send an alert by email. This workflow is a great way to power on your environment after a maintenance procedure that requires shutdown.

Web Tasks

Template	Description
Archive old IIS log files	Reads list of IIS servers and archives log files which are older than 90 days.
List application pools	Lists all application pools on a list of servers and sends them in the form of an HTML report by email.
Monitor and recover IIS	Checks the status of the IIS service on a list of servers, and restarts the service in case it is stopped. You can use this process as a scheduled task to monitor the service's status on a regular basis or as part of a larger workflow when handling an incident.
Monitor and recover web site	Monitors the availability of a URL, by searching for a specific phrase that indicates the site as available. In case the site is detected as unavailable, a set of activities is performed. You can schedule this process to run on an hourly basis to monitor your top websites, and alert the relevant personnel in case of unavailability.
Monitor list of URLs	Monitors the availability of a list of URLs and sends an availability report to the Admin user.
Monitor URL according to IP address	Monitors the availability of a website from a specific IP address. Use this process to check the availability when you are using a load balancer. The process checks if the website is available, and in case it is not, the IP address the host is configured to run from is sent to the Admin user. In case the website is available, the process edits the URL's IP address in the c:\windows\system32\drivers\etc\hosts file to check the website's availability in the next interval from another address.
Start application pools	Lists all application pools on a host and starts every application pool which is not already started.