Managing scripts

Active IQ Unified Manager 9.8

NetApp
April 16, 2024

Table of Contents

Managing scripts

You can use scripts to automatically modify or update multiple storage objects in Unified Manager. The script is associated with an alert. When an event triggers an alert, the script is executed. You can upload custom scripts and test their execution when an alert is generated.

The ability to upload scripts to Unified Manager and run them is enabled by default. If your organization does not want to allow this functionality because of security reasons, you can disable this functionality from **Storage Management** > **Feature Settings**.

How scripts work with alerts

You can associate an alert with your script so that the script is executed when an alert is raised for an event in Unified Manager. You can use the scripts to resolve issues with storage objects or identify which storage objects are generating the events.

When an alert is generated for an event in Unified Manager, an alert email is sent to the specified recipients. If you have associated an alert with a script, the script is executed. You can get the details of the arguments passed to the script from the alert email.

The script uses the following arguments for execution:

- `-eventID`
- `-eventName`
- `-eventSeverity`
- `-eventSourceID`
- `-eventSourceName`
- `-eventSourceType`
- `-eventState`
- `-eventArgs`

You can use the arguments in your scripts and gather related event information or modify storage objects.

Example for obtaining arguments from scripts

```
print "$ARGV[0] : $ARGV[1]\n"
print "$ARGV[7] : $ARGV[8]\n"
```

When an alert is generated, this script is executed and the following output is displayed:

```
-eventID : 290
-eventSourceID : 4138
```

Adding scripts

You can add scripts in Unified Manager, and associate the scripts with alerts. These scripts are executed automatically when an alert is generated, and enable you to obtain information about storage objects for which the event is generated.

Before you begin

- You must have created and saved the scripts that you want to add to the Unified Manager server.
- The supported file formats for scripts are Perl, Shell, PowerShell, and `.bat` files.

Platform on which Unified Manager is installed	Supported languages
VMware	Perl and Shell scripts
Linux	Perl and Shell scripts
Windows	PowerShell, Perl, and .bat scripts

  - For Perl scripts, Perl must be installed on the Unified Manager server. For VMware installations, Perl 5 is installed by default and scripts will support only what Perl 5 supports. If Perl was installed after Unified Manager, you must restart the Unified Manager server.
  - For PowerShell scripts, the appropriate PowerShell execution policy must be set on the Windows server so that the scripts can be executed.

  If your script creates log files to track the alert script progress, you must make sure that the log files are not created anywhere within the Unified Manager installation folder.

- You must have the Application Administrator or Storage Administrator role.

About this task

You can upload custom scripts and gather event details about the alert.

If you do not see this capability available in the user interface it is because the functionality has been disabled by your administrator. If required, you can enable this functionality from **Storage Management** > **Feature Settings**.

Steps

1. In the left navigation pane, click **Storage Management** > **Scripts**.
2. In the **Scripts** page, click **Add**.
3. In the **Add Script** dialog box, click **Browse** to select your script file.
4. Enter a description for the script that you select.
5. Click **Add**.

Deleting scripts

You can delete a script from Unified Manager when the script is no longer required or valid.

Before you begin

- You must have the Application Administrator or Storage Administrator role.
- The script must not be associated with an alert.

Steps

1. In the left navigation pane, click **Storage Management** > **Scripts**.
2. In the **Scripts** page, select the script that you want to delete, and then click **Delete**.
3. In the **Warning** dialog box, confirm the deletion by clicking **Yes**.

Testing script execution

You can verify that your script is executed correctly when an alert is generated for a storage object.

Before you begin

- You must have the Application Administrator or Storage Administrator role.
- You must have uploaded a script in the supported file format to Unified Manager.

Steps

1. In the left navigation pane, click **Storage Management** > **Scripts**.
2. In the **Scripts** page, add your test script.
3. In the left navigation pane, click **Storage Management** > **Alert Setup**.
4. In the **Alert Setup** page, perform one of the following actions:

To…	Do this…
Add an alert	a. Click **Add**. b. In the Actions section, associate the alert with your test script.
Edit an alert	a. Select an alert, and then click **Edit**. b. In the Actions section, associate the alert with your test script.

5. Click **Save**.
6. In the **Alert Setup** page, select the alert that you added or modified, and then click **Test**.

The script is executed with the “-test” argument, and a notification alert is sent to the email addresses that were specified when the alert was created.

Enabling and disabling the ability to upload scripts

The ability to upload scripts to Unified Manager and run them is enabled by default. If your organization does not want to allow this activity because of security reasons, you can disable this functionality.

Before you begin

You must have the Application Administrator role.

Steps

1. In the left navigation pane, click **General** > **Feature Settings**.
2. In the **Feature Settings** page, disable or enable scripting by choosing one of the following options:

If you want to…	Then do this…
Disable scripts	In the **Script Upload** panel, move the slider button to the left.
Enable scripts	In the **Script Upload** panel, move the slider button to the right.

Supported Unified Manager CLI commands

As a storage administrator you can use the CLI commands to perform queries on the storage objects; for example, on clusters, aggregates, volumes, qtrees, and LUNs. You can use the CLI commands to query the Unified Manager internal database and the ONTAP database. You can also use CLI commands in scripts that are executed at the beginning or end of an operation or are executed when an alert is triggered.

All commands must be preceded with the command `um cli login` and a valid user name and password for authentication.

CLI command	Description	Output
`um cli login -u <username> [-p <password>]`	Logs in to the CLI. Because of security implications, you should enter only the user name following the “-u” option. When used in this manner you will be prompted for the password, and the password will not be captured in the history or process table. The session expires after three hours from the time of login, after which the user must login again.	Displays the corresponding message.
`um cli logout`	Logs out of the CLI.	Displays the corresponding message.
`um help`	Displays all first level subcommands.	Displays all first level subcommands.
`um run cmd [ -t <timeout> ] <cluster> <command>`	The simplest way to run a command on one or more hosts. Mainly used for alert scripting to get or perform an operation on ONTAP. The optional timeout argument sets a maximum time limit (in seconds) for the command to complete on the client. The default is 0 (wait forever).	As received from ONTAP.
`um run query <sql command>`	Executes an SQL query. Only queries that read from the database are allowed. Any update, insert, or delete operations are not supported.	Results are displayed in a tabular form. If an empty set is returned, or if there is any syntax error or bad request, it displays the appropriate error message.

CLI command	Description	Output
`um datasource add -u <username> -P <password> [ -t <protocol> ] [ -p <port> ] <hostname-or-ip>`	Adds a datasource to the list of managed storage systems. A datasource describes how connections to storage systems are made. The options -u (username) and -P (password) must be specified when adding a datasource. The option -t (protocol) specifies the protocol used to communicate with the cluster (http or https). If the protocol is not specified, then both protocols will be attempted The option -p (port) specifies the port used to communicate with the cluster. If the port is not specified, then the default value of the appropriate protocol will be attempted. This command can be executed only by the storage admin.	Prompts for the user accept the certificate and prints the corresponding message.
`um datasource list [ <datasource-id>]`	Displays the datasources for managed storage systems.	Displays the following values in tabular format: `ID Address Port, Protocol Acquisition Status, Analysis Status, Communication status, Acquisition Message, and Analysis Message.`
`um datasource modify [ -h <hostname-or-ip> ] [ -u <username> ] [ -P <password> ] [ -t <protocol> ] [ -p <port> ] <datasource-id>`	Modifies one or more datasource options. Can be executed only by the storage admin.	Displays the corresponding message.
`um datasource remove <datasource-id>`	Removes the datasource (cluster) from Unified Manager.	Displays the corresponding message.
`um option list [ <option> .. ]`	Lists all the options that you can configure using the `set` command.	Displays the following values in tabular format: `Name, Value, Default Value, and Requires Restart.`
`um option set <option-name>=<option-value> [ <option-name>=<option-value> ... ]`	Sets one or more options. The command can be executed only by the storage admin.	Displays the corresponding message.

CLI command	Description	Output
`um version`	Displays the Unified Manager software version.	`Version ("9.6")`
`um lun list [-q] [ -ObjectType <object-id>]`	Lists the LUNs after filtering on the specified object. -q is applicable for all commands to show no header. ObjectType can be lun, qtree, cluster, volume, quota, or svm. For example: `um lun list -cluster 1` In this example, "-cluster" is the objectType and "1" is the objectId. The command lists all the LUNs within the cluster with ID 1.	Displays the following values in tabular format: `ID and LUN path`.
`um svm list [-q] [ -ObjectType <object-id>]`	Lists the storage VMs after filtering on the specified object. ObjectType can be lun, qtree, cluster, volume, quota, or svm. For example: `um svm list -cluster 1` In this example, "-cluster" is the objectType and "1" is the objectId. The command lists all the storage VMs within the cluster with ID 1.	Displays the following values in tabular format: `Name and Cluster ID`.
`um qtree list [-q] [ -ObjectType <object-id>]`	Lists the qtrees after filtering on the specified object. -q is applicable for all commands to show no header. ObjectType can be lun, qtree, cluster, volume, quota, or svm. For example: `um qtree list -cluster 1` In this example, "-cluster" is the objectType and "1" is the objectId. The command lists all the qtrees within the cluster with ID 1.	Displays the following values in tabular format: `Qtree ID and Qtree Name`.

CLI command	Description	Output
`um disk list [-q] [-ObjectType <object-id>]`	Lists the disks after filtering on the specified object. ObjectType can be disk, aggr, node, or cluster. For example: `um disk list -cluster 1` In this example, "-cluster" is the objectType and "1" is the objectId. The command lists all the disks within the cluster with ID 1.	Displays the following values in tabular format `ObjectType and object-id.`
`um cluster list [-q] [-ObjectType <object-id>]`	Lists the clusters after filtering on the specified object. ObjectType can be disk, aggr, node, cluster, lun, qtree, volume, quota, or svm. For example:`um cluster list -aggr 1` In this example, "-aggr" is the objectType and "1" is the objectId. The command lists the cluster to which the aggregate with ID 1 belongs.	Displays the following values in tabular format: `Name, Full Name, Serial Number, Datasource Id, Last Refresh Time, and Resource Key.`
`um cluster node list [-q] [-ObjectType <object-id>]`	Lists the cluster nodes after filtering on the specified object. ObjectType can be disk, aggr, node, or cluster. For example: `um cluster node list -cluster 1` In this example, "-cluster" is the objectType and "1" is the objectId. The command lists all the nodes within the cluster with ID 1.	Displays the following values in tabular format `Name and Cluster ID.`
`um volume list [-q] [-ObjectType <object-id>]`	Lists the volumes after filtering on the specified object. ObjectType can be lun, qtree, cluster, volume, quota, svm, or aggregate. For example: `um volume list -cluster 1` In this example, "-cluster" is the objectType and "1" is the objectId. The command lists all the volumes within the cluster with ID 1.	Displays the following values in tabular format `Volume ID and Volume Name.`

CLI command	Description	Output
`um quota user list [-q] [-ObjectType <object-id>]`	Lists the quota users after filtering on the specified object. ObjectType can be qtree, cluster, volume, quota, or svm. For example: `um quota user list -cluster 1` In this example, "-cluster" is the objectType and "1" is the objectId. The command lists all the quota users within the cluster with ID 1.	Displays the following values in tabular format `ID, Name, SID and Email`.
`um aggr list [-q] [-ObjectType <object-id>]`	Lists the aggregates after filtering on the specified object. ObjectType can be disk, aggr, node, cluster, or volume. For example: `um aggr list -cluster 1` In this example, "-cluster" is the objectType and "1" is the objectId. The command lists all the aggregates within the cluster with ID 1.	Displays the following values in tabular format `Aggr ID, and Aggr Name`.
`um event ack <event-ids>`	Acknowledges one or more events.	Displays the corresponding message.
`um event resolve <event-ids>`	Resolves one or more events.	Displays the corresponding message.
`um event assign -u <username> <event-id>`	Assigns an event to a user.	Displays the corresponding message.
`um event list [ -s <source> ] [ -S <event-state-filter-list>.. ] [ <event-id> .. ]`	Lists the events generated by the system or user. Filters events based on source, state, and IDs.	Displays the following values in tabular format `Source, Source type, Name, Severity, State, User and Timestamp`.
`um backup restore -f <backup_file_path_and_name>`	Restores a MySQL database backup using .7z files.	Displays the corresponding message.

Description of script windows and dialog boxes

The Scripts page enables you to add scripts to Unified Manager.

Scripts page

The Scripts page enables you to add your custom scripts to Unified Manager. You can associate these scripts with alerts to enable automatic reconfiguration of storage objects.

The Scripts page enables you to add or delete scripts from Unified Manager.

Command buttons

- **Add**

  Displays the Add Script dialog box, which enables you to add scripts.

- **Delete**

  Deletes the selected script.

List view

The list view displays, in tabular format, the scripts that you added to Unified Manager.

- **Name**

  Displays the name of the script.

- **Description**

  Displays the description of the script.

Add Script dialog box

The Add Script dialog box enables you to add scripts to Unified Manager. You can configure alerts with your scripts to automatically resolve events that are generated for storage objects.

You must have the Application Administrator or Storage Administrator role.

- **Select Script File**

  Enables you to select a script for the alert.

- **Description**

  Enables you to specify a description for the script.

Copyright information

Trademark information