Monitor drivers with a Driver Dashboard

Open Horizons Magazine 2017 Q2

by Andreas Fuhrmann, SKyPRO AG, Switzerland

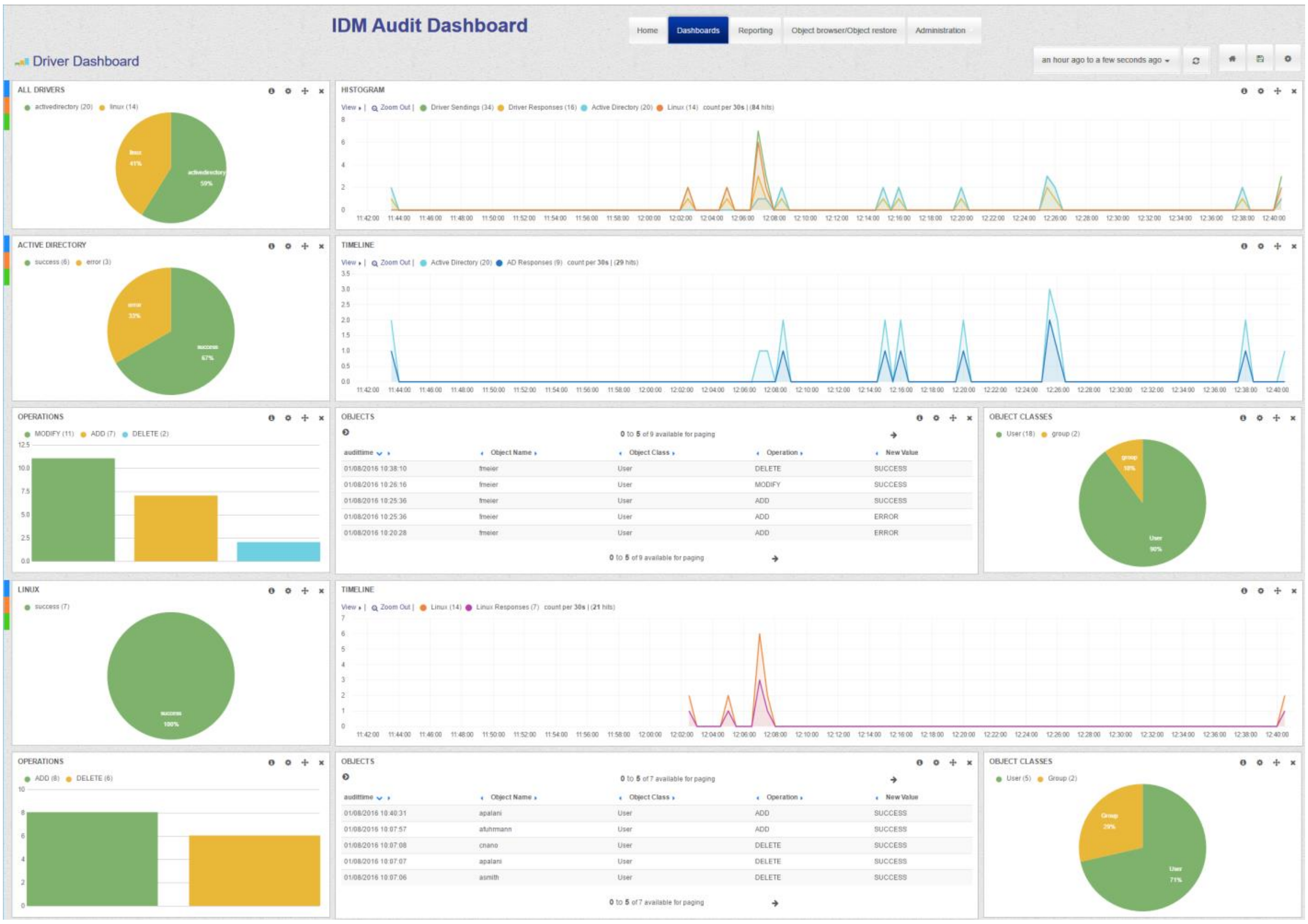
As we all know one of the key features of Micro Focus Identity Manager is its powerful and flexible real time provisioning engine. Whatever object, attribute or permission you want to synchronize into or from an integrated system, whichever interface you're going to use, ancient csv files or modern REST or SOAP, IDM does it reliable, fast and with ease. BUT when it comes to the question, when has a specific modification been received in the IDM Vault and was it propagated successfully by all drivers to the connected systems, it might cause some headache. With the help of the Driver Dashboard, that is part of the Audit & Compliance Dashboard, we solve this puzzle.

The real world

Assume you have a complex IDM solution in place with over 50 or even 100 connected systems. Furthermore, imaging you have a full grown Identity & Access Governance solution and the HR application is connected with your Identity Vault. A new employee is born and synchronized into your Identity Vault. Based on the HR information several business roles will be assigned to this new employee. These business roles have child roles and the inheritance ends up with several permission roles and resources, which will be assigned to the new employee. Because of all these inherited and assigned resources the employee is entitled for several accounts and permissions in divers application and systems.

If all goes the way it should, and believe me in most cases it does, our IDM drivers will provision this user to all these applications and systems, create the accounts with all attribute values and assign all the specific access rights the user is entitled for. But in this case the employee calls the help desk complaining that he cannot log into a critical financial application and other systems. So you have the challenge to check what went wrong in your provisioning process.

This is the moment where the Driver Dashboard comes in place. The Driver Dashboard is one of the many dashboards that come with the IDM Audit & Compliance Dashboard.



OBJECTS

0 to 5 of 9 available for paging

audittime	Object Name	Object Class	Operation	New Value
01/08/2016 10:38:10	fmeier	User	DELETE	SUCCESS
01/08/2016 10:26:16	fmeier	User	MODIFY	SUCCESS
01/08/2016 10:25:36	fmeier	User	ADD	SUCCESS
01/08/2016 10:25:36	fmeier	User	ADD	ERROR
01/08/2016 10:20:28	fmeier	User	ADD	ERROR

0 to 5 of 9 available for paging

OBJECTS

0 to 5 of 7 available for paging

audittime	Object Name	Object Class	Operation	New Value
01/08/2016 10:40:31	apalani	User	ADD	SUCCESS
01/08/2016 10:07:57	afuhrmann	User	ADD	SUCCESS
01/08/2016 10:07:08	cnano	User	DELETE	SUCCESS
01/08/2016 10:07:07	apalani	User	DELETE	SUCCESS
01/08/2016 10:07:06	asmith	User	DELETE	SUCCESS

0 to 5 of 7 available for paging

Figure 1: The Driver Dashboard

What does the Driver Dashboard show?

The Driver Dashboards shows in detail every event, that has been processed by the subscriber or publisher channel of each individual driver, that has been Driver Dashboard enabled. At the top, it presents a real-time summary of all events processed by dashboard enabled drivers (see figure 2). In the upper left corner, you see a pie chart representing the number of events handled by each driver.

The histogram on the right shows each individual driver event, that has been processed by the drivers in a timeline. In our example, we have integrated three different drivers in the driver dashboard, the publisher channel of an HR driver and the subscriber channel of an Active Directory and a Linux driver.

The dashboard differs between number of events send thru the channel and the number of responses received from the target system. In case a target system does not respond, you'll see more send than receive events.

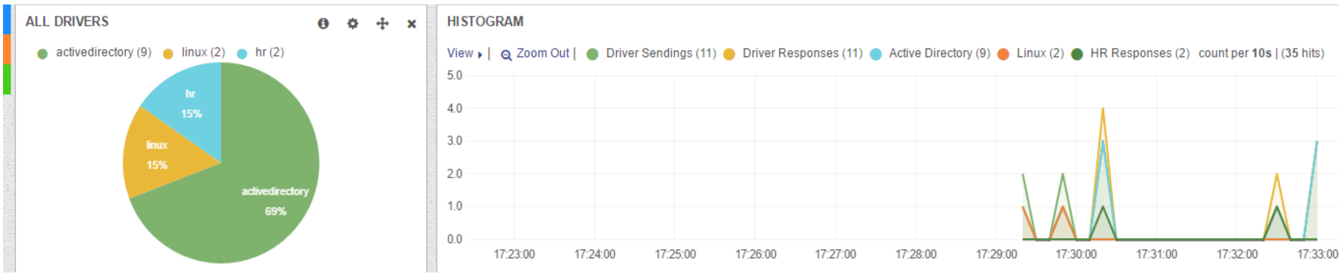
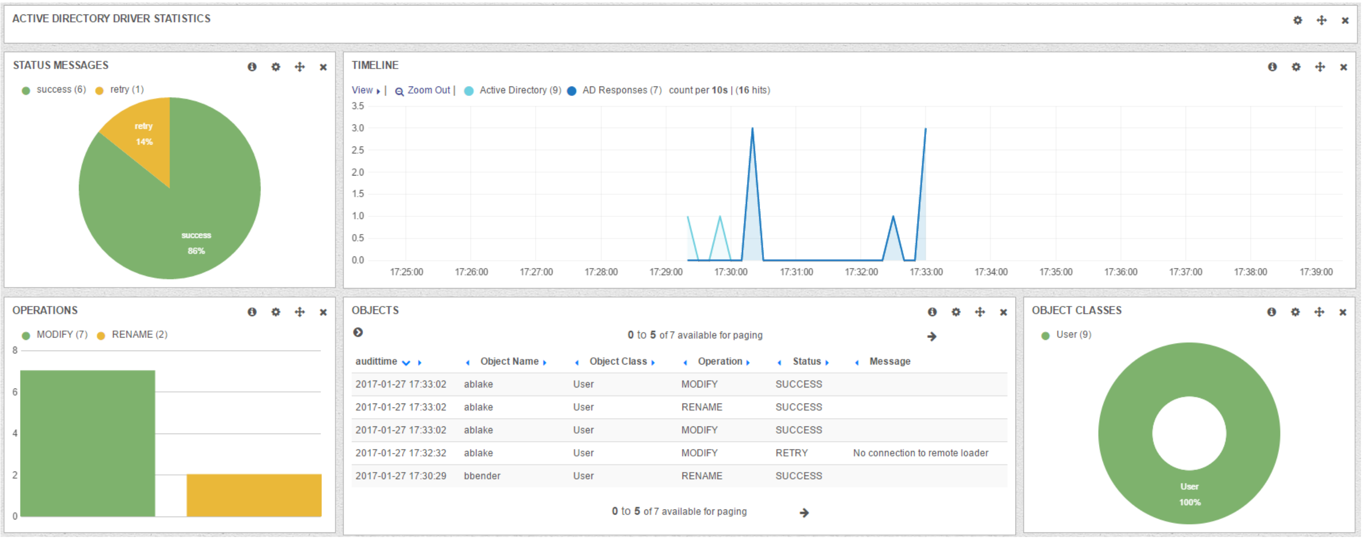


Figure 2: The Driver Dashboard Summary

Below the summary, each driver has its own presentation in the dashboard. In figure 3 we see a presentation of an Active Directory driver. The pie chart in the upper left shows the number of successes, errors, warnings or retries issued by the driver. In this example, we have a retry due to a lost connection to the remote loader. In the upper right, we again have the histogram of all events processed by this specific driver.

The lower left shows the number of different events like add, modify, rename, move or delete handled by the driver. The table in the middle is one of the most interesting parts. It shows the details to every event including the responses from the connected system and its messages. In this example, we see the “RETRY” caused by a restart of the remote loader and the message “No response from remote loader”.



0 to 5 of 7 available for paging

audittime	Object Name	Object Class	Operation	Status	Message
2017-01-27 17:33:02	ablake	User	MODIFY	SUCCESS	
2017-01-27 17:33:02	ablake	User	RENAME	SUCCESS	
2017-01-27 17:33:02	ablake	User	MODIFY	SUCCESS	
2017-01-27 17:32:32	ablake	User	MODIFY	RETRY	No connection to remote loader
2017-01-27 17:30:29	bbender	User	RENAME	SUCCESS	

0 to 5 of 7 available for paging

Figure 3: The Active Directory Driver Dashboard

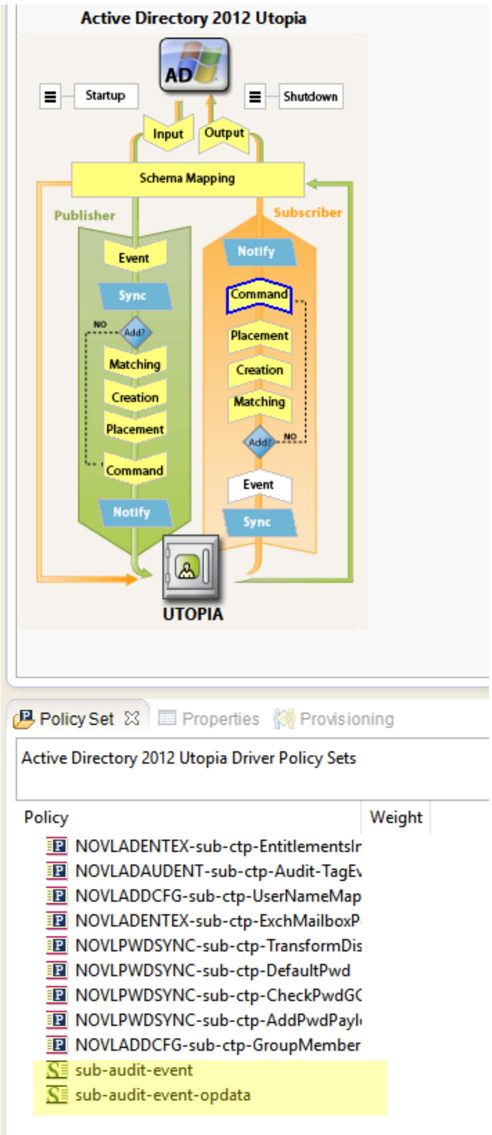
Enabling a driver for the Driver Dashboard

As mentioned before, before you can monitor a driver in the Driver Dashboard you have to enable the driver. This is done by copy and paste three predefined policies into the subscriber or publisher channel, depending which channel you want to audit. Of course, you can audit both channels simultaneously. All necessary policies are included in the package.

As you see in figures 4 and 5 we have to add two Command Transform Policies and one Input Transform Policy to your driver enabling them to create the necessary information for the Driver Dashboard. Actually, these policies create a special acdAudit object in you eDirectory. We provide the needed schema file to do the schema extension. These objects will be created in a special organizational unit. The audit driver, that comes with the Audit & Compliance Dashboard will process these objects and synchronize the information to the elastic search server. The acdAudit objects will be deleted in eDirectory after they have been successfully processed by the audit driver.

Fell free to adjust the preconfigured policies to your requirements. You can add additional information to be send to the elastic search indexes, you can even add the complete XML document, if you like. You can also adjust the default driver dashboards to show this additional information.

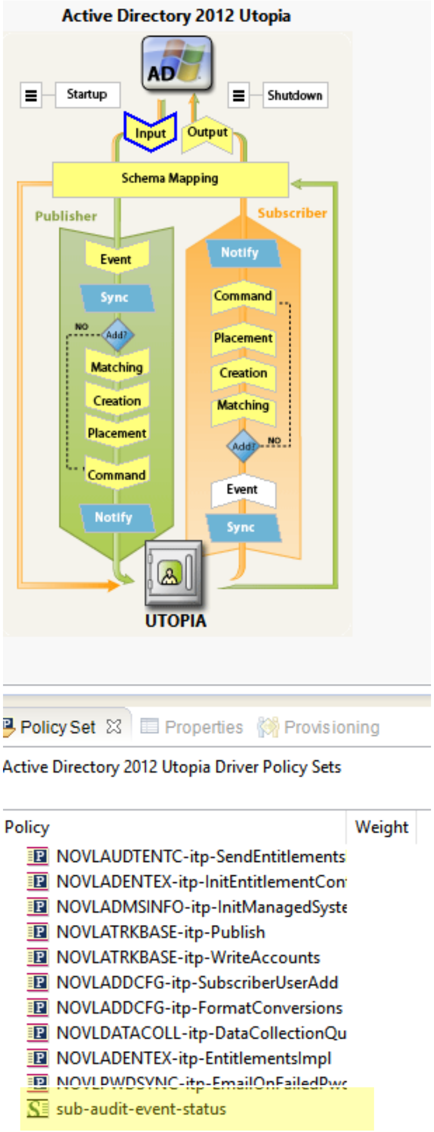
To conclude with the audit & compliance dashboard we provide you with a very comprehensive toolset to build your own driver dashboards to monitor all your IDM drivers real time. If you like to add more information to the dashboard you have everything in place to do so in a very short time.



Active Directory 2012 Utopia Driver Policy Sets

Policy	Weight
NOVLADENTEX-sub-ctp-EntitlementsIr	
NOVLADAUDENT-sub-ctp-Audit-TagEv	
NOVLADDCFG-sub-ctp-UserNameMap	
NOVLADENTEX-sub-ctp-ExchMailboxP	
NOVLPWDSYNC-sub-ctp-TransformDis	
NOVLPWDSYNC-sub-ctp-DefaultPwd	
NOVLPWDSYNC-sub-ctp-CheckPwdGC	
NOVLPWDSYNC-sub-ctp-AddPwdPaylo	
NOVLADDCFG-sub-ctp-GroupMember	
sub-audit-event	
sub-audit-event-opdata	

Figure 5: two additional Command Transform Policies



Active Directory 2012 Utopia Driver Policy Sets

Policy	Weight
NOVLAUDTENTC-itp-SendEntitlements	
NOVLADENTEX-itp-InitEntitlementCon	
NOVLADMSINFO-itp-InitManagedSyste	
NOVLATRKBASE-itp-Publish	
NOVLATRKBASE-itp-WriteAccounts	
NOVLADDCFG-itp-SubscriberUserAdd	
NOVLADDCFG-itp-FormatConversions	
NOVLDATACOLL-itp-DataCollectionQu	
NOVLADENTEX-itp-EntitlementsImpl	
NOVLPWDSYNC-itp-EmailOnFailedPwc	
sub-audit-event-status	

Figure 4: one additional Input Transform Policy