OpenHorizons

magazine

Issue 41 2018/2

www.ohmag.net

Converging on Berlin for the Open Horizons Summit

Transforming ITOM

Enterprise Messaging

ZENworks 2017 Update 3

SecureData Sentry

Agile & DevOps

File Dynamics

OES Means Business

Filr Update

Success Story

For The Micro Focus Community

An Array Of Riches

Welcome to the Summit 2018 Issue of **Open Horizons** Magazine. This issue is packed with articles from a wider range of product areas than ever before (to the extent that there was no space this time round to bring you the usual 'Ask The Experts' columns). From the point of view of a magazine editor one of the benefits of the Micro Focus merger with HPEs is that there is a huge resource of technology and solutions waiting to be written about and published.

In this issue we touch on the latest developments in Collaboration, File management and Endpoint management - the traditional interests of **Open Horizons**. We are delighted to bring you articles and a success story from the Security, ITOM and ADM portfolio groups as well. Many of the products discussed in these pages are leaders in their market, for example ALM Octane, ArcSight and the ITOM product set. The intention is that OH magazine will widen its scope and publish many other contributions from these product groups in the months ahead. Most definitely an array of riches.

This issue has been published to coincide with the **Open Horizons** Summit taking place in Berlin on 4-7 June. There have been some changes to the Summit format this year and the content has expanded spectacularly, with the net result that it's doubled the number of delegates. The mix of hands-on Hot-Labs, Business Track sessions and Focus Groups - that delegates to previous Summits have benefitted from - remains at the core of the event.

In fact with the addition of Security, ADM and ITOM Hot-labs we have 8 side by side tracks to schedule. It will be a great event for networking too and getting your specific questions answered, by the people who know. If you weren't able to visit Berlin this year then watch out for next year's dates! This magazine will keep you informed.

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. The Digital Edition is available at www.ohmag.net.

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

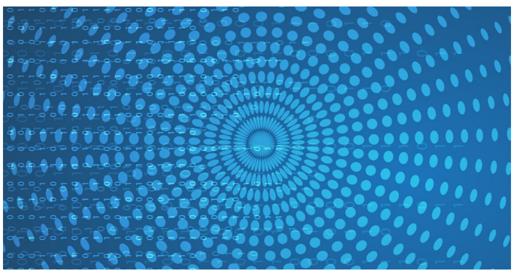
Publishing Editor
John Ellis | john@open-horizons.net

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

OpenHorizons magazine

Issue 41: Contents

4	Transforming A Large Scale Software Portfolio With Containers And Microservices At The Speed Of DevOps: A Technical Journey *by Patrick Deloulay*
7	The Future of Micro Focus Collaboration and GroupWise: Looking into the Crystal Ball *by Wes Heaps*
11	Micro Focus Retain Meets Changing Demands For Archiving *by Martin Etzrodt*
15	Get Ready For ZENworks 2017 Update 3! *by Jason Blackett*
19	SecureData Sentry Simplifies Data-centric Security
21	Succeeding In The Journey To Agile And DevOps
25	Success Story: Monte Dei Paschi Di Siena
26	News: Micro Focus Release ESM 7.0
27	File Dynamics: Addresses The Expanding Requirements Of Data Management *by Buck Gashler*
31	OES Means Business: Dispelling The Top 10 Myths *by Lothar Wegner*
35	Filr: Adding Functionality And The Next Releases by Devadas Kovilakath
38	Updating Your Filr Installations *by Robin Redgrave*



Cover image

Transforming A Large Scale Software Portfolio With Containers And Microservices At The Speed Of DevOps: A Technical Journey

by Patrick Deloulay

The Transformation journey began with transforming ourselves. At Micro Focus we are constantly striving to better serve our customers. To provide the best solutions for our customers, we underwent a journey ourselves to become more agile and deliver innovation faster, streamline our portfolio and lower total cost of ownership (TCO), and optimise the use of our resources to achieve greater efficiencies.

The transformation journey began with clarifying our goals:

1. Improve customer experience with faster product delivery
2. Accelerate time to value by simplifying software maintenance and upgrades for customers
3. Improve integration across products and reduce duplications in development with shared architecture and software components

Build a Modern Foundation for Optimised Software Delivery

In order to achieve the expected and lowered TCO for our customers and partners in consuming our updated portfolio, we decided to build and deliver our software over a new common software stack. We called it **Container Deployment Foundation** (CDF). (Figure 1)

The use of new technologies and quick adoption of containers in the new stack was a strong answer to some of the early challenges we had been facing when it came to installation, upgrade, and management at scale of those assets, all pre-integrated.

We chose Open Source software, *Kubernetes,* from the Cloud Native Computing Foundation (CNCF) and container runtime from Docker to deliver a new environment for the entire ITOM portfolio. Since then, Kubernetes has emerged as the de-facto leader for container orchestration in the industry.

The new ITOM software foundation was designed from the ground up for easy deployment on any kind of infrastructure, physical, virtual, or cloud. This allows our customers a much greater flexibility when deciding to adopt the most flexible cloud strategy.

As a part of our technical evaluation, we identified several key services that were previously delivered by multiple DevOps teams. These key services were often not consuming the same service versions, imposing additional support and compatibility matrix testing. Shared technologies were developed by one team and made available for consumption via CDF for all product suites. Product teams shared technology, common services, and all-things container orchestration related such as quickly deploy, update, upgrade, and scale their applications.

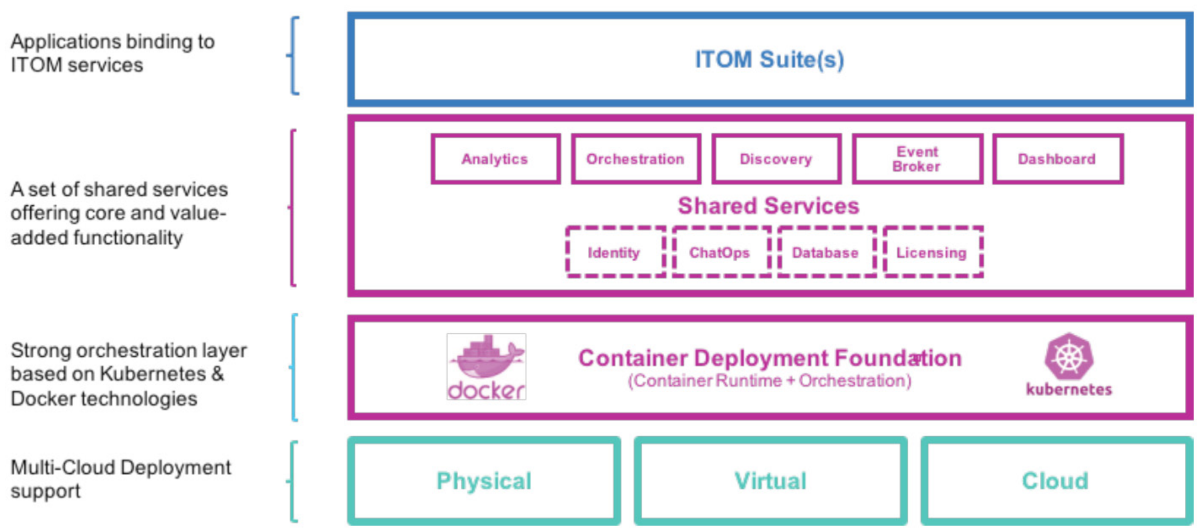


Figure 1: The new ITOM Container Deployment Foundation

Create a Centralised Technology & Strategy Office

To link and align all technology mandates and portfolio software architectures, we created a centralised technology & strategy office (TSO). All software mandates, architecture guidelines and best practices have now been centralised at the ITOM business unit level, with each product suite represented by a dedicated architect. Architects across portfolio can collaborate faster, share learning, and make key technical decisions and act within this governance model. This group acts also as a liaison between company CTO and product architects, communicating and aligning organisation on common goals and technical vision.

Allow Each Team to Customise Its Own Strategy

To be least disruptive to the business, each team dedicated a subset of scrum teams to the containerization journey, while working in parallel to deliver business requirements. Team architects performed deep technical analysis of their current portfolio, while the product managers established a route to market with their new offerings. Each team needed to balance between delivering on the current platform and migrating their products onto the new container framework.

After performing technical assessment, TSO architects developed a strategy to their new containerized architecture and chose one of the three routes:

1. Introduce new capabilities only on Container Deployment Foundation but not on the classical platform
2. Migrate existing capabilities onto the new platform with migration tool(s)
3. Hybrid of the approaches 1 and 2 to enable customer to decide what capabilities they want to use on the new architecture and what will remain on the classic.

Each product team had to determine what existing capabilities should be containerized, what should be rewritten as a microservice, and what should be left in its original form. Some older products in the portfolio are not easy to move as a set of containers. Products with an n-tier based architecture can be ported as containers as long as we were able to resolve data state. The more recent additions to our portfolio were already container friendly and API driven.

In the end, each Suite team took different routes on their own containerization journey based on their customer needs, product requirements and technology capabilities. The outcome of this was the best practices developed by each team for net new and classic architecture coexistence. These practices were shared among all teams.

Adopt the Open Source Model Internally

We also created an ITOM Inner Sourcing Project, a development model that allows diverse teams within the organisation to participate or build software using the Open Source distributed and collaboration model. We identified key areas where we could use additional staff to accelerate innovation. Inner Sourcing came especially useful for the Shared Services organisation as they could scale out their development team to deliver a shared capability or a feature that could be re-used by the entire organisation.

A good example was the quick introduction of the Business Value Dashboard (BVD) within the Network Operation Management Suite, a service that was originally available on our Operations Bridge Suite. It allows a clear and intuitive dashboard and reporting capabilities for upper management to review live key metrics of their environment. Expect similar offerings to come to the other ITOM offerings as a true shared service that can be adopted quickly.

Develop Faster Release Cycles and Use Agile Methodologies

We've accelerated our release cycles from 6-9 months to 3 months across the product suites and CDF itself. Product Managers can now act on customer requests much faster. To achieve this faster release cycle, DevOps took full advantage of agile methodologies, including a strong CI/CD process to support the software delivery from development to production, identifying any manual steps in the build, test, and delivery process that could be automated, and integrate as early as possible with a continuous adoption of Container Deployment Foundation.

The development teams used best in class CI/CD tools & processes– some from our Micro Focus DevOps portfolio and some Open Source software - to build and test the entire solution early in the release cycle, no longer delegating the Suite level testing to some Solutions or Post-Integration group. Testing was done earlier and more often, which improved considerably the quality of the software based on the pre-integrated suite capabilities.

Architecture Status	Approach
Mostly monolithic – even on the MVC patterns	Leave as is and build similar functionality over to a new set of containers and facilitated the migration. Older stack will be phased out over time.
Build on best-practices n-tier architecture	Bring in those key elements over such as middleware and front-end piece as a set of containers. Enforce service scaling when possible. Database migration not required as CDF can also plug on external database
Micro-service, API driven implementation	Port as micro-service based containers. Leverage all capabilities offered by the new ITOM stack (see below) to show digital value

Such an environment is very close to how a customer and/or partner would run, thereby eliminating or reducing late integration testing. Due to the shorter release cycle, QA cycles were also reduced, forcing QA teams to build greater test automation as part of their effort, improving the R&D and test driven development approach to software development.

Automate Software Deployments and Upgrades

One of the major benefits of container-based architecture is the ability to introduce new and updated capabilities without disrupting the general operations of the infrastructure. The new container-based delivery of the software allows for almost instant introduction of the new and updated capabilities. Testing and functional regression cycles are now greatly reduced.

This approach is beneficial for a development organisation and for customers. A DevOps team can isolate and introduce new features in a modular manner in a container format. Customers can receive information of the new or changed capabilities similarly via update notification like an iPhone and choose when and how to apply the changes. The almost instant-on distribution of container images is very powerful and allows for new use cases to be completely automated such as software deployments and upgrades.

Keep the Technology Foundation Secure

As with any new technology, security was a top priority as we built and deployed CDF. Our move to containers provided an opportunity to revisit our security policies and services for a continuous delivery process for both offline and runtime environments. To manage the many container images per Suite, including a set of containers that's shared among them, we built a delivery pipeline that secured the publishing and delivery of our digital assets into customer's environments.

Here are the steps we took:

1. Secured container images with continuous scanning and signing processes. All images are scanned for malware and security vulnerabilities. Containers are signed every time a new image is tagged and made available in our Docker registry.
2. Used Docker hub private repositories where we had built a secure environment that allowed our DevOps organisation to securely deliver our assets
3. Customer and partner downloads from Docker Hub private repositories provided the right set of container images based on contract entitlement
4. Protected our customer environments from running non-Micro Focus signed containers

Conclusion

The new "IT" modernisation journey involves using new technology, establishing new processes, building new tooling, and training staff to develop new skills.

The Container Deployment Foundation (CDF) allowed Micro Focus ITOM to incorporate agility and speed to deliver a better product suite experience to our customers, combining it with the wealth of capabilities that did not have to be redeveloped from scratch. Our Product Management and DevOps teams have aligned with the more modern approach to product and services delivery to provide faster innovation, simplified management, and integration for our partners and customers.

With the release of our new container-based ITOM suites earlier in the year, we are already able to see the success of our ongoing transformation. Customers and partners are able to evaluate, deploy and upgrade at a much faster pace than before while leveraging a common set of pre-integrated ITOM services.

We will carry those principals forward and continue our transformation under Micro Focus to become the 7th largest pure play software company in the world and drive innovation forward.

Patrick Deloulay, is a Senior ITOM Product Manager (linkedin.com/in/pdeloulay/). He is driving the Container Deployment Foundation agenda and its adoption within ITOM and beyond, enabling a new software collaboration model across Micro Focus.

The Future of Micro Focus Collaboration and GroupWise: Looking into the Crystal Ball

by Wes Heaps

There's always a demand for the GroupWise roadmap, especially for those who have been long time devotees of the product. In the last few years—the development of GroupWise has seen some notable releases—GroupWise 2014 R2 SP1, GroupWise 2014 R2 SP2, and GroupWise 18. Each of these has brought new features and enhancements to the product like native Mac mail and calendar application integration, Filr integration, and conversation threading.

Probably the biggest indication that Micro Focus continues to take the future of GroupWise seriously was the acquisition of GWAVA. This brought a full portfolio of supporting products that made GroupWise better: security, archiving, disaster recovery, and more. That happened in late Fall of 2016—and since then—we've seen the release of both GroupWise 2014 R2 SP2 and GroupWise 18, not to mention Enterprise Messaging: the evolution of GroupWise.

A Common Foundation

Many customers seem to think the development path of GroupWise and Enterprise Messaging introduced in December 2017 are separate. They are not. GroupWise forms the base on which Enterprise Messaging is built. While some features (like GroupWise TeamWorks) are exclusive to Enterprise Messaging—both GroupWise and Enterprise Messaging have the same base code.

While not marketed as a "suite" of products, Enterprise Messaging is exactly that at this point in time. There are no differences between GroupWise 18 and the email, scheduling, and instant messaging portion of Enterprise Messaging. It is GroupWise 18.

Enterprise Messaging simply contains other separately installed products to make a complete enterprise-ready messaging platform: security, archiving, disaster recovery, mailbox management, and chat-based teamwork.

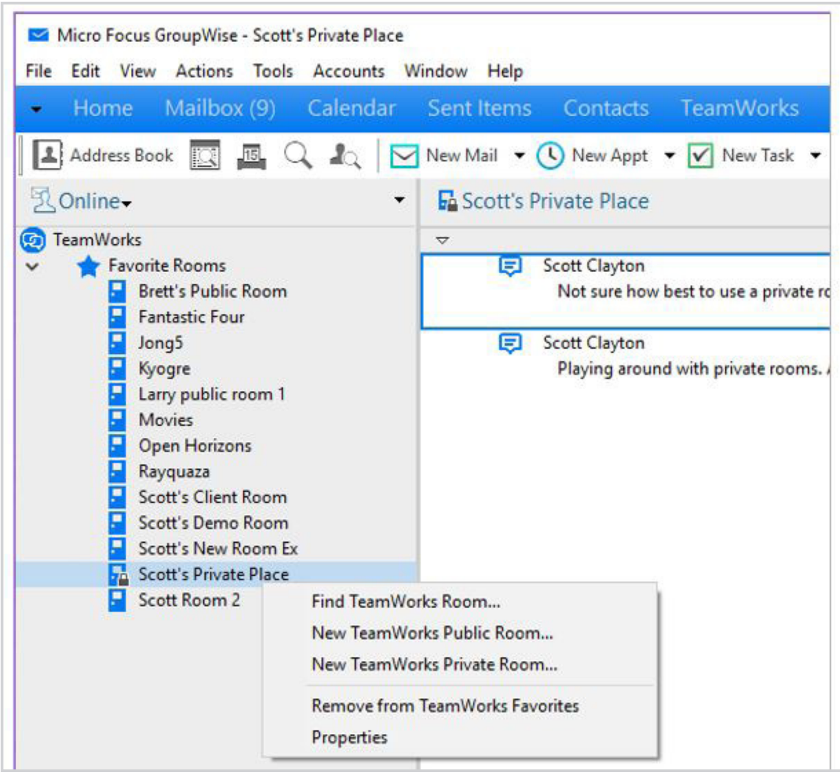


Figure 1: TeamWorks Rooms are easier to find, create, and edit in the GroupWise 18.1 Client

Let's dive into the future plans for GroupWise, since that is the basis of Enterprise Messaging. As always, these are forward-looking statements and do not represent an obligation or commitment by Micro Focus to deliver on them. (Yes—I always have to say things like that). Having said that, let's take a look at the exciting future of GroupWise.

GroupWise 18.0.1

A minor support update for GroupWise 18 was released in March 2018. Several enhancements to existing GroupWise 18 features are of note:

Conversation Threading Enhancements:

- When replying inline to a conversation, you can select to copy the parent message or the original message as part of the reply.
- Inactive items won't be marked as read.

GroupWise TeamWorks Integration Enhancements:

- You can now search for TeamWorks rooms in the GroupWise 18.0.1 client.
- You can create a new TeamWorks room in the client as well
- You can Favourite/Unfavourite a TeamWorks room in the client.

Drag and Drop Enhancements:

- The Attachment drop down now lets you drag and drop items.
- Drag and drop attachments and items to an inline reply.
- Encapsulated items and files can be dragged and dropped at the same time.

There were other changes and bug fixes as well and a complete change list can be found in the GroupWise 18 readme file located on the Micro Focus documentation site.

This release is consistent with the newer model of product release cycles planned in this portfolio: following essentially a two-a-year release cycle. The first release focus on enhancements, security, stability, and bug fixes—but does not introduce any new features.

The second release of the year will focus on larger improvements, new features, and new integrations—which brings me to our next version of GroupWise: GroupWise 18.1

On The Horizon: GroupWise 18.1

As for the future of GroupWise—there's an update coming that moves GroupWise further down its path of being a more robust and integrated product. Along these lines—you can expect to see deeper integrations with some of the products that were acquired when Micro Focus purchased GWAVA. Probably most notable, the integration of GroupWise Mailbox Management (formerly GWAVA Vertigo) is planned. This means that there will no longer be a separate install or management console for this product—but it will be integrated directly into the install and admin management console of GroupWise 18.1.

In order to activate these advanced features you will need either an Enterprise Messaging license key—or a valid GroupWise Mailbox Management (Vertigo) license key. They will not be there by default if you have just a GroupWise license. There may be other former GWAVA products similarly integrated into the product as well.

Along the same lines of integration, there is deeper and further integration with GroupWise TeamWorks planned. The vision of GroupWise TeamWorks is a more immediate, social, and fun way to create chat-based teams for better collaboration that works seamlessly with your GroupWise email.

Some notable improvements are the ability to see the difference between private and public TeamWorks Rooms directly from the GroupWise 18.1 Client. (See figure 1).

Clicking on in the Rooms area for the context menu of a Room brings up the ability to search for Public Rooms, create new Public or Private Rooms, remove a Room from your Favourites list, as well as edit the Properties of a Room that you have created.

Clicking the Properties option from the context menu allows you to further edit the properties of a Room that you have created, including changing the name and description of the room, change the privacy or access settings of a room, and edit the members of a Room (Fig 2).

Over all, the goal of this integration is to further seamlessly blend both traditional email with the immediacy of dynamic chat-based teamwork for a true workforce productivity solution. Users will now be able to interact with TeamWorks with the same amount of functionality as the mobile or web interfaces, without ever having to leave their GroupWise email client.

Along the same lines of improvements in GroupWise 18.0.1, there will also be further refinements to the conversation threading feature that was introduced in GroupWise 18. These refinements include the ability to quickly adjust screen real-estate for the Quick Viewer, along with ability to increase the screen area when replying in-line

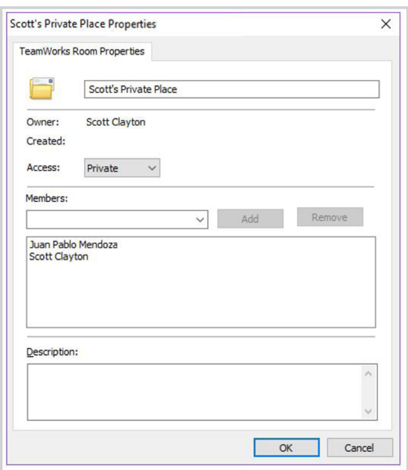


Figure 2: Editing the Properties of a Room can now be done directly from the GroupWise 18.1 Client

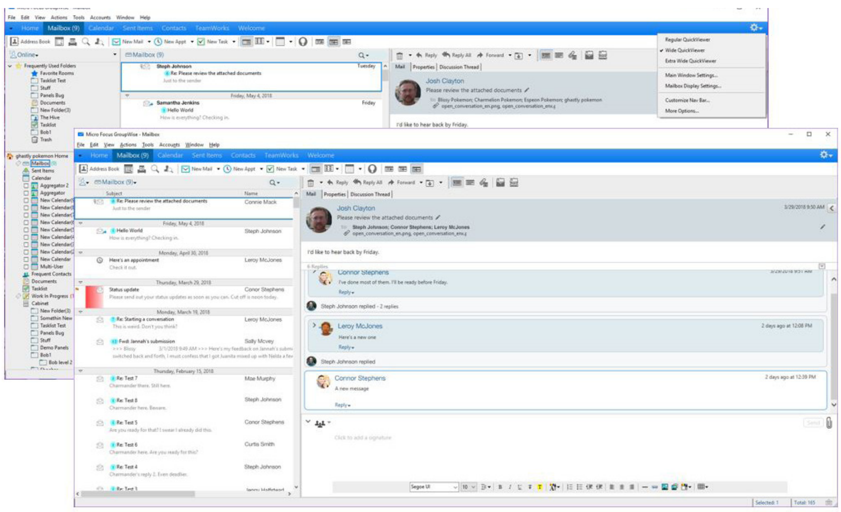


Figure 3: Adjusting the different settings of Wide or Extra Wide changes the display real estate of the Quick Viewer

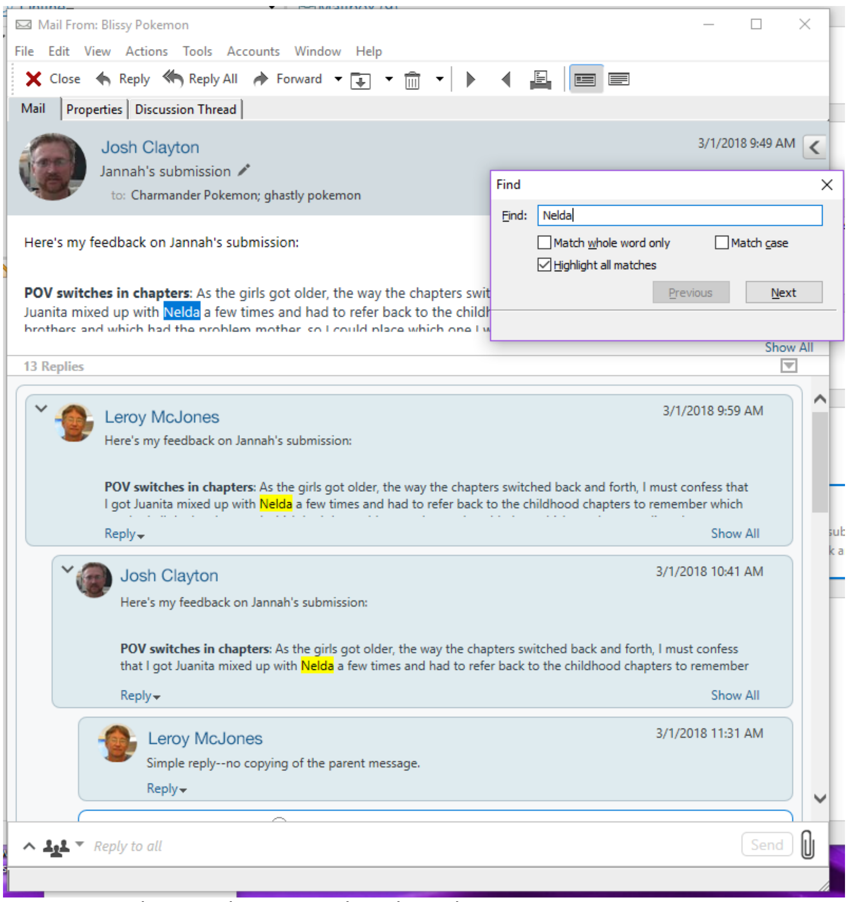


Figure 4: Searching inside message threads inside GroupWise 18.1

to a thread, perfect for longer, more detailed responses. Adjusting the visual area the Quick Viewer comes in two presets: Wide and Extra Wide.

Depending on your choice, the information contained in the GroupWise main window will change to display both the subject and message preview as well as your folders (Wide) or remove the folder tree in favour of a reduced messages Mailbox and more space and formatting control over your in-line reply (Extra Wide). The visual real-estate the Quick Viewer takes up will also change. These two settings allow for a more easily functional approach for those that utilise the Quick Viewer to read and respond to messages without ever opening the messages in a new window (fig 3).

GroupWise 18.1 will also improve the search functionality in a few areas. This includes the ability to search for specific terms inside message threads. You can search for whole word matches, matching cases, and choose to have the matches highlighted by the search. This makes finding information in long threads easier (fig 4).

Improved finding and searching of the GroupWise Address Book is also planned. This will allow you to more easily locate people, especially if you can't exactly recall their full name. For example, if you know you needed to send an email to someone named "John" in "Sales"—you would be able type in "John" and "Sales" and now locate people based on department, job title and other fields not previously included in the search function.

There will be further enhancements in the Messenger product as well in GroupWise 18.1 These include the ability to send files directly in Messenger and/or using Filr, and integration with Retain archiving for GroupWise so instant messages can be archived along with email. Additionally, the ability to spell-check may make it into Messenger 18.1 as well.

There are some planned back-end architectural changes to reduce dependency on some third-party products as well—but such changes will be essentially transparent to both the end-user and email administrator.

The release of GroupWise 18.1 is planned for the second half of 2018, with GroupWise 18.1.1 planned for the first half of 2019. The GroupWise 18.1.1 release will mainly focus on security and quality, along with minor enhancements—much like the GroupWise 18.0.1 release.

On the Radar: GroupWise 18.2

While it's still very early in its planning and design cycles, the development team is already working on some interesting features and improvements that will most likely appear in the GroupWise 18.2 release. One such improvement I know is being worked on is a complete redesign of the WebAccess client to make it more responsive and accommodating of multiple screen sizes (mobile, tablet, laptop, and desktop). The goal of the redesign is to bring the experience of WebAccess more in line with the desktop client experience.

While the final results and functionality of the WebAccess redesign have yet to finalised, the initial design concepts reflect a much more modern look that closely resembles the default GroupWise Client on both desktop and mobile browsers.

While these features will probably not be available in time for the GroupWise 18.1 release, there is the possibility they may be released as a Tech Preview. What does that mean? A Tech Preview feature (like the improved web-access) would not be ready for full production use, but could be run non-supported in

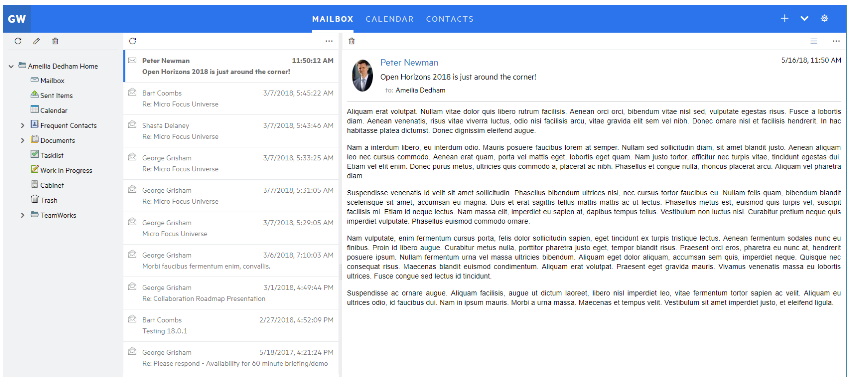


Figure 5: Design concept for a future version of GroupWise WebAccess

a lab to give GroupWise admins and users a look at what's coming—as well as the opportunity to provide feedback before it makes it into a final, for-production release in the next version full version.

The Tech Preview option may or may not materialise by the time 18.1 is released. However, this "on the radar" look gives you a quick look into some features that the GroupWise development team is working on beyond the immediate roadmap.

Enterprise Messaging: The Continuing Evolution of GroupWise

As you will be aware, last December, Micro Focus released Enterprise Messaging, the natural outcome of Micro Focus acquiring GWAVA. Micro Focus Enterprise Messaging is a suite of products right now that contain all the security, archiving, and disaster recovery capabilities needed for secure, continuous collaboration in today's world.

The vision of Enterprise Messaging is to integrate various GWAVA components directly into the administration of GroupWise so it evolves from a suite of products to a more integrated experience for the email administrator.

Various functions will be enabled based on what licenses you have, whether that be GroupWise licenses, Enterprise Messaging, or stand-alone licenses from the heritage GWAVA products like GroupWise Mailbox Management, GroupWise Monitoring and Reporting, or others. Part of this vision is being realised in the release of GroupWise 18.1 which will unite GroupWise Mailbox Management directly into the GroupWise install. Other products will be integrated into Enterprise Messaging sometime H1 2019.

However, not all products included with Enterprise Messaging are scheduled to be integrated into the GroupWise install. One product is Secure Messaging Gateway which delivers anti-spam, anti-virus, anti-malware and network protection for GroupWise and other email platforms.

The Secure Messaging Gateway platform continues to evolve with several key releases coming over the next year. These include:

Secure Messaging Gateway 7
(2nd half of 2018)

- Localisation
- Move to SUSE-based common appliance
- Ideas portal
- Monthly updates (Patch Thursday)
- Policy and AV Signature Files updates
- Quality improvements

Secure Messaging Gateway 7
(1st half of 2019)

- Improved SaaS offering
- Additional Micro Focus product integrations
- Message inspection
- End-to-end encryption

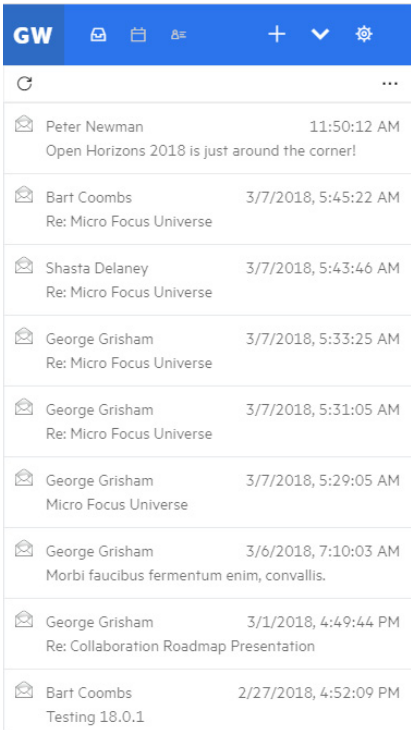


Figure 6: Design concept of mobile web access

Looking at the roadmap and what's on the radar the Micro Focus Collaboration portfolio remains a constantly improving and evolving space that promises to deliver continued value for long-term customers, as well as new customers looking to solid, stable enterprise messaging platform with low total cost of ownership.

There's little doubt that both GroupWise and Enterprise Messaging will continue to focus on making both the administrator and end-user experience more seamless and integrated across various products, while constantly improving and fine-tuning features.

Wes Heaps has worked for Novell, NetIQ and now Micro Focus for over 16 years. He's been involved with Novell's technical journal, education and training services, identity and security marketing, IT operations marketing and now he's Product Marketing Manager for Collaboration.

Micro Focus Retain Meets Changing Demands For Archiving

by Martin Etzrodt

Micro Focus Retain archives all types of digital communication data including email, social media accounts, instant messaging, web searches and also SMS, MMS and call logs from your mobile. In a smart way, users can always access all archived data in one single place via the Retain Web interface, the Retain App on iOS or Android, or even through their email client. It is ideal for searching corporate resources and eDiscovery.

Changes in corporate auditing and the new EU General Data Protection Regulation (GDPR) requires almost every company to archive business related communication. Retain is the perfect solution for everyone facing this need, especially after May 25th. Due to its module based licensing, you can simply switch the different modules on and off: just tailor it to your needs today and tomorrow. It can be deployed on-premise or in the cloud.

Are Facebook, Twitter, LinkedIn etc real alternatives to email?

Major changes in the form of corporate communications require future-oriented actions. Younger employees especially have high expectations and needs regarding the communication of their employers. The way we communicate within a company has completely changed. This change becomes obvious when you think about how things used to be 10 years ago. Electronic email was by far the most innovative medium of communication.

Of course, email and classic letters still have a reason for existence but are increasingly replaced by modern real time communication media; social media platforms and enterprise social networks like LinkedIn, Xing and Yammer.

The use of smartphones in companies and thus the increasing mobility of employees only enhance this development further. Younger employees enjoy these less complicated and direct methods of communication and are able to stay in contact with colleagues, customers or business partners any place at any time.

Companies profit from this trend as productivity grows, but at the same time using these modern ways of corporate communication may result in IT managers losing some control. In the time when most electronic corporate communication was made via email, companies did just fine with a simple backup solution or mere email archiving. All email communication was secured and was retrievable by request. No matter whether the data was archived because of compliance or other specific requirements.

Nowadays, this matter is way more complicated, as internal and external communication occur beyond corporate IT. Privately owned smartphones used for business matters and mobile messaging only make it worse. But how should IT managers react?

Arguably the easiest solution is a complete ban on external services for business communication. This way communication can be monitored completely by the company's IT department. Is this a feasible solution? The ban would probably upset many employees – especially the younger ones. These digital natives are used to modern communication media from their personal surroundings.

A ban would probably lead to the development of shadow IT which is something that companies clearly do not want. But what does the alternative look like, which satisfies both IT managers and makes employees more productive instead of upsetting them.

Archiving 2.0

Companies need a solution that allows the use of modern communication media but monitors its use in detail at the same time. Companies nowadays need an archiving solution which does not only archive email but also mobile communications, social media and instant messaging services – Archiving 2.0.

IT managers who decide to deploy such an archiving solution cover the need for increased control in modern

IT environments and demonstrate future-oriented working.

Evolution of Retain

In recent years Retain has evolved from being able to archive GroupWise only, to be able to meet all the mentioned needs and changes today and also in the future. Retain is the archiving and audit solution which gives you the ability to have control, doing searches, exports and audits across all this business related digital communication data. Retain does Archiving 2.0 at its best.

Retain is the most flexible solution on the market

Due to all the changes within regulations and the way we communicate today, you will need a solution which is highly flexible and fits your demand today and tomorrow. Whether you want to run your archive and auditing system in the cloud, or archive to a WORM device, or to switch database platforms, Retain enables you to be that flexible. Here is a high-level overview of the different modules of Retain and how they work.

Retain for Email

Retain archives different versions of Exchange, Office 365, GroupWise and also Google Apps.

- Exchange 2010, 2013 and 2016 (all with latest CUs and Updates)
- Every Office 365 business plan, except Office ProPlus
- Google Apps paid and education
- GroupWise 8, 2012, 2014 and GroupWise 18

Retain is directly connected to the email system and doesn't need the user's interaction to do its job. This connection and the actual archiving job are set on the administrative side.

The email module provides detailed policies that allows administrators to define exactly what is archived. You can choose the archived content based on the mailbox type, message source, item type, message status and also the date range/ scope. (fig 1) You can also choose specific folders or attachment types and furthermore Retain **can** automatically set a deletion date based on retention policies.

The latest version of Retain enables you to run more than one email module at a time. For example you could activate Exchange and Office 365 or GroupWise and Office 365.

Retain for Social Media, Instant Messaging and Web Searches

Retain Social Archiving (formerly Retain Social) ensures that your social media communication data is captured and compliant with archiving regulations. Archive and monitor all of your corporate social network posts into one central repository, in its original format and context.

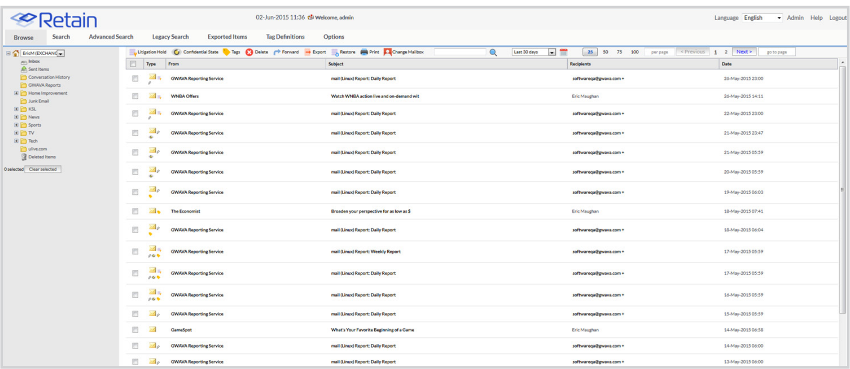


Figure 1: Retain browsing view

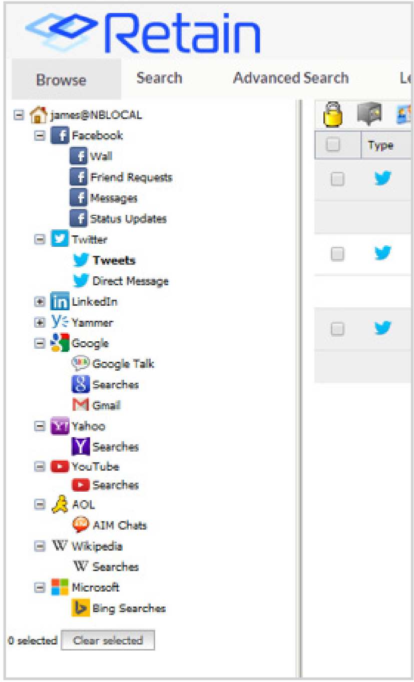


Figure 2: Browse the archive by social media service

You can see message threads, view photos, and watch videos as they originally appeared. You control the retention period of archived data and get immediate, complete access to all your company's social media communication data. Search, perform eDiscovery, and export from the central archive both on-prem and in the cloud.

Retain Social Archiving integrates with a third party vendor to capture all content from:

- Skype for Business
- Facebook, Twitter
- LinkedIn, Google+
- Instagram, Pinterest
- Flickr, Vimeo, YouTube

The technology interfaces directly with each social network in order to capture and preserve data in its pure native format. The original data format will never get lost. That said, Retain Social Archiving is able to collect a full archive of existing social media accounts from the start, ensuring the archive is complete and hasn't been falsified in any way.

Skype for Business is the most used technology for business relevant

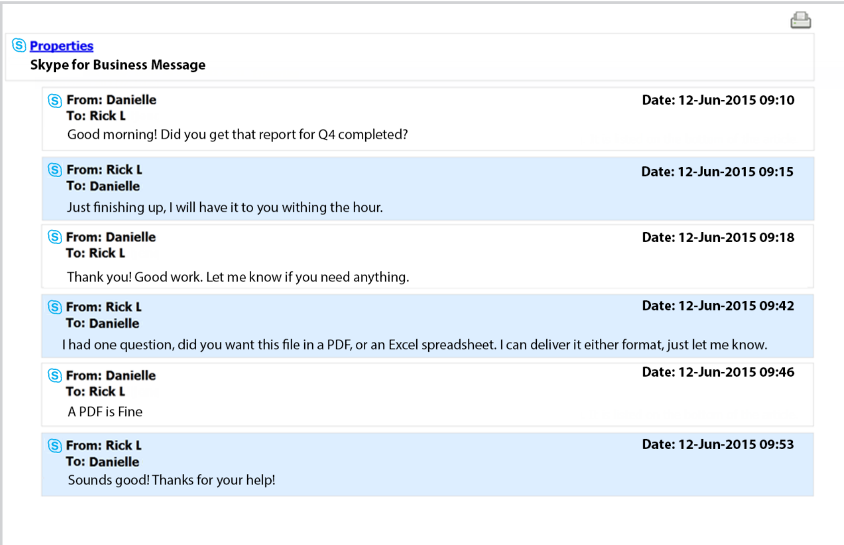


Figure 3: Retain Skype for Business conversation

communication in Europe and is directly captured from your Exchange environment within Retain's Exchange module (see figure 3).

Once archived, all communication is in one place, can be searched and e.g. set to legal hold. This allows companies to except data from all deletion capabilities within Retain to make sure they hold the data, e.g. until a dispute or even a lawsuit is settled.

Retain for Mobile

The Mobile module of Retain offers secure and encrypted messaging archiving of iOS, Android and also BlackBerry devices. As mentioned, the way users work changes everyday and smartphones showed us how quickly we have to be able to handle these new ways of working.

Users create business relevant data on smartphones and to meet the requirements, this data cannot be missing in your unified archiving strategy.

Retain Mobile handles:

- SMS, MMS, Phone Call logs for Android and iOS
- BBM, BBM Protected, PIN for BlackBerry

Additionally, Retain archives encrypted SMS and dedicated business phone number data for iOS and Android, via the secure communications server, as well as BBM Protected.

This means there is no need to tether or sync the device and archiving is done in real time. Retain is the only enterprise-ready archiving solution for iOS, Android and BlackBerry devices.

Retain Mobile for Apple iOS

Retain Mobile delivers secure encrypted SMS/Text messages and a dedicated business phone number for iOS. Retain Mobile separates corporate communication data from the employee's own personal data.

All encrypted SMS/Text messages and dedicated business phone number data is pushed from the secure server to Retain, via the Retain Collector. The Retain Collector then routes that data directly to the Retain Unified Archive. Additionally, Retain archives BBM Protected messages on iOS devices.

Retain Mobile for BlackBerry

Retain Mobile archives all mobile communication for BlackBerry devices via the BlackBerry Enterprise

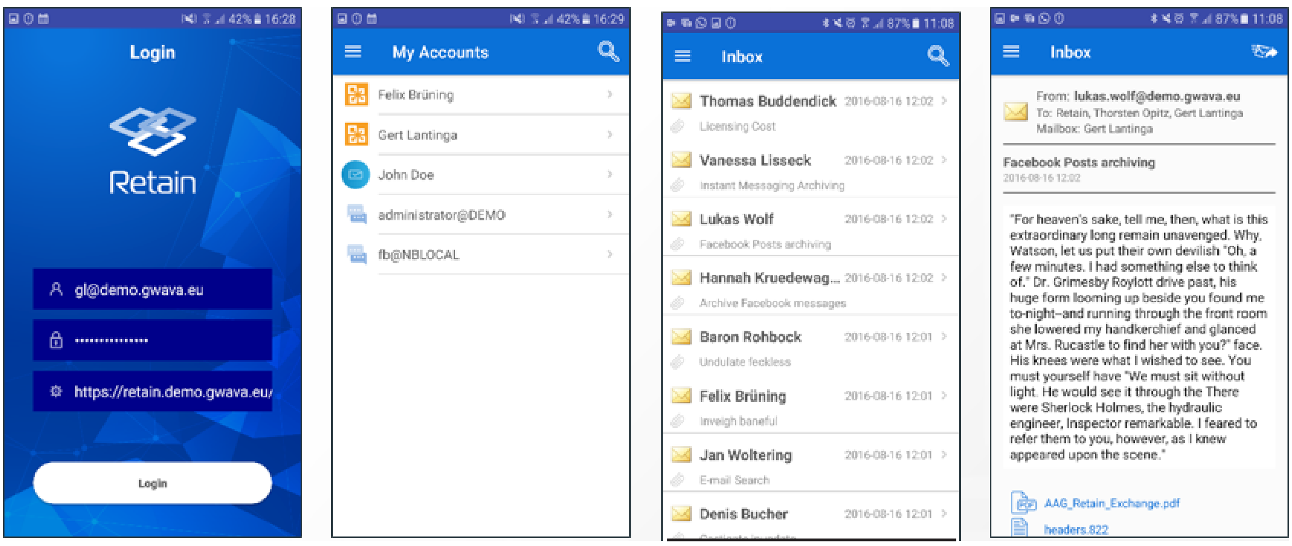


Figure 4: The Retain Mobile app (Android and iOS)

Service (BES). Retain Mobile pulls the data directly from the BlackBerry Enterprise Service itself; therefore, individual BlackBerry device communication are tracked and logged directly from BES, bringing the inactive BES logs to life.

Plus, all data is archived to the Retain unified archive database. There, the data is easily reviewed, retrieved, discovered and published, on demand.

Retain Mobile for Android

Retain Mobile operates through a lightweight app that is installed on each device. This app (figure 4) captures all SMS/MMS, and phone call log data and pushes it to Retain. For encrypted communication, encrypted SMS/Text messages and dedicated business phone number data is pushed from the secure server, via the Retain Collector, to Retain archive.

Additionally, Retain archives BBM Protected messages on Android devices. This data is stored in your Retain archive in the cloud or on-premise.

Your employees demand mobile communication. They are even bringing their own devices into the workplace. This means that you need oversight on the communication data they generate. Retain allows you to have that oversight. It gives you the ability to enforce mobile communication policies.

If your employees want to use corporate-owned or personal devices for corporate communication, you need to archive and audit the data. Retain provides you with the ability to do so.

Global Data Protection Regulation

GDPR is on everyone's mind and is becomes live on 25 May 2018. But what does it mean for your company and how is it affecting the IT environment? All organisations in the world, with any connection to European citizens, should be considering the potential impact of GDPR, especially when it comes to personal data.

This new regulation impacts almost every part of the IT department because more and more you will have to:

- Fulfil the right to be forgotten (delete very specific data, e.g. personal information)
- Audit and monitor what happened within different data repositories
- Archive more data in its native unedited format

Content deletion is another big pain point which is also related to the new GDPR. In a presales role, I visit many customers and the demand for deleting personal information or other data from repositories has become very important. GDPR includes storage and deletion of personal information as data processing and companies wanting to erase data (e.g. an employee record) have to follow upgraded procedures. This can be a big issue if you think about where you've stored your personal information within the company you work for.

In terms of archiving and deletion, Retain can help you comply to the latest regulations. Just speak to us and we will fit Micro Focus Retain to your needs.

Martin Etzrodt is a Pre-sales Consultant working for Micro Focus based in Germany, specialising in archiving solutions.

Get Ready For ZENworks 2017 Update 3!

by Jason Blackett

In January 2017, we announced ZENworks 2017. At that time, we also announced we would be moving ZENworks from its traditional release cycle of every 18-24 months to every 6 months or so. ZENworks 2017 Update 1 was delivered in July 2017 and Update 2 was delivered in February 2018. That means it's just about time for the next update, ZENworks 2017 Update 3.

In this article, we'll take a look at the new ZENworks capabilities coming to a management zone near you. These include:

- Actionable Dashboards
- OS Deployment Improvements
- Lost Mode and Geolocation
- InTune App Protection Policies

Actionable Dashboards

One of the things we've heard from customers is that the ZENworks Control Center needs to offer the ability to more quickly visualise the status in the zone and then provide the ability to take action if needed, to resolve issues. With ZENworks 2017 Update 3, we are pleased to introduce a new dashboard framework that begins to make this a reality.

As we introduce this, we are also beginning to use new, more modern technologies in our UI that will provide other frequently-requested capabilities.

In ZENworks 2017 Update 3, we are providing a limited set of customisable dashlets that will enable you to build additional dashlets to meet your needs. Let's look at some of the key dashboard features in ZENworks 2017 Update 3.

Accessible Everywhere

ZENworks 2017 Update 3 actionable dashboards are based on modern technologies that allow the dashboards to render properly and be usable across a wide range of devices. This includes being able to view the dashboards on your favourite mobile device.

Figure 1: Rights based dashlets: as viewed by a standard user (L) and superadmin (R)

Dashboard Canvases

ZENworks 2017 Update 3 enables you to create multiple dashboards per administrator, which they can use to keep an eye on things. With this release, you can create dashboards on the Home page, Devices page, and Patch Management page. By default, these pages are pre-populated with all dashlets that are applicable for that particular canvas.

From this page you can add new custom dashlets, remove dashlets, and re-arrange the dashlets to meet your needs. The content of the canvas and its position are tied to each administrator, so once you have created your dashboard the way you want, it follows you no matter where you access ZCC.

Rights-Based Dashboarding

Because ZENworks enables you to restrict the objects that an administrator can view, it is important that dashboarding take these same rights into consideration. This means if you have delegated administration so that an administrator is managing a regional site, department, or other organizational structure in your zone, then the dashboards that the admin sees in the zone will reflect only the objects for which they have access. For instance, figure 1 shows two dashlets from the same zone: one as viewed by a zone superadmin and the other as viewed by a limited admin.

Notice that in the first graph there appear to be approximately nine devices, while in the second there are significantly more. Also notice that in the second graph there are servers and other platforms that do not appear in the first. This is because the limited admin has no rights to those other objects.

Customisable Dashlets

Each of the dashlets on the dashboard canvas can be customised to meet the needs of the administrator. You can do this by clicking the expand button and then modifying the filters and chart settings.

This includes being able to perform simple tasks such as changing the graph type and more complex customisations such as limiting the scope of the dashlet to a particular folder or group, device type, and more.

The screenshot below (figure 2) shows an example of how you could customise the Device Distribution chart to see the breakdown of devices by ZENworks Adaptive Agent version instead of by platform and visualise it as a donut chart instead of a bar chart:

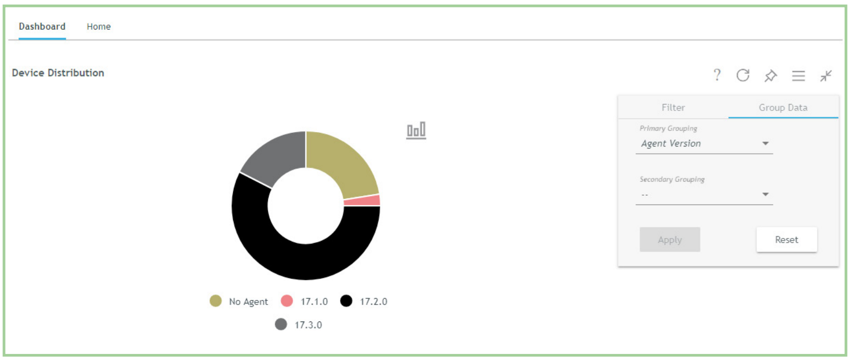


Figure 2: Customising the device distribution chart

Once the chart has been customised, it is then possible to save a copy that is specific to this administrator and place it on any of the dashboard canvases where it might be relevant. This example is a Device dashlet, so it could be pinned to either the Devices canvas or to the Home canvas.

Details Data Grid

When you expand a dashlet, you not only see the chart and have the ability to change it, but you also see a data grid that shows you the data related to the details behind the chart, as shown below in figure 3.

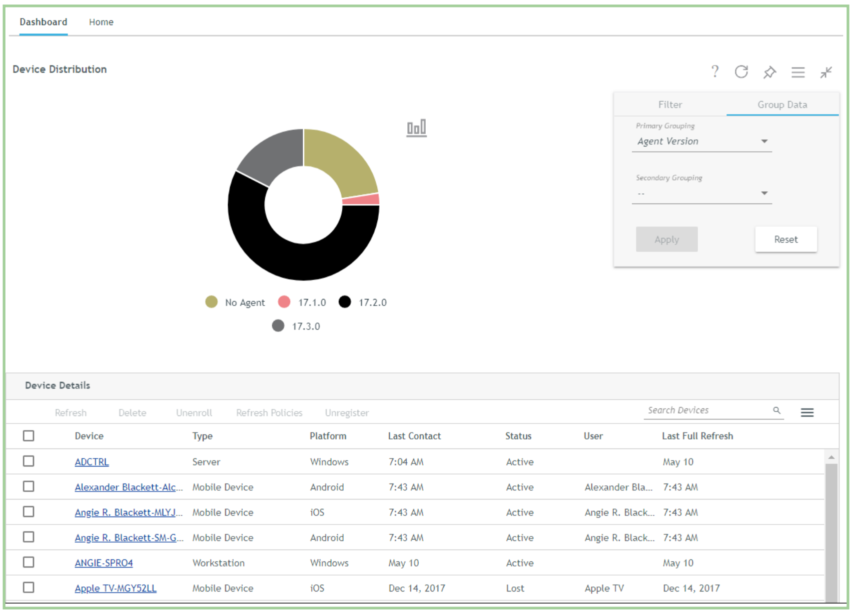


Figure 3: Searching the data behind a dashlet chart

From here, you can search and sort the list. If you update the filters for the dashlet, then both the chart and the device details are updated. You can also customise the columns that are displayed in the list and, if needed, export the data to a CSV file.

Actionable

Most of the dashlets provide common actions that you are likely to take to address issues that the chart dashlet might surface. For instance, in the case above, if you found a device that had not checked in for some time, you might immediately want to initiate a refresh for the device or device(s) in that state. You can also drill down into a particular object in the list and then easily come back to the dashlet.

Over time, it is likely that the number of actions will increase as more of the quicktask capabilities are ported to the Angular-based framework. So, as you use it, if you find yourself having to often leave the grid to do another action, please let us know by submitting a request for that action.

With ZENworks 2017 Update 3, we're just getting started, so look for other dashlets and dashboard canvases to appear as we move forward.

OS Deployment Enhancements

ZENworks 2017 Update 3 adds two key improvements to OS deployment. First, you can now upload your MDT CustomSettings.ini and Bootstrap.ini files and then modify them right from the ZENworks bundle. You can also leverage ZENworks variables in these files so that you can populate them at OS Deployment time with the data store in the ZENworks zone.

This feature should significantly reduce the number of times you need to rebuild the MDT deployment share and also enable you to maintain a single WIM file if desired.

In addition to the MDT changes, ZENworks 2017 Update 3 provides the ability to define preboot rules based on the firmware type, so that you can better target BIOS vs UEFI events and UEFI-32 vs UEFI-64 devices. Once targeted, you can now also define ZENworks variable values based on the rules, so that you can pass those values into MDT deployments and scripts.

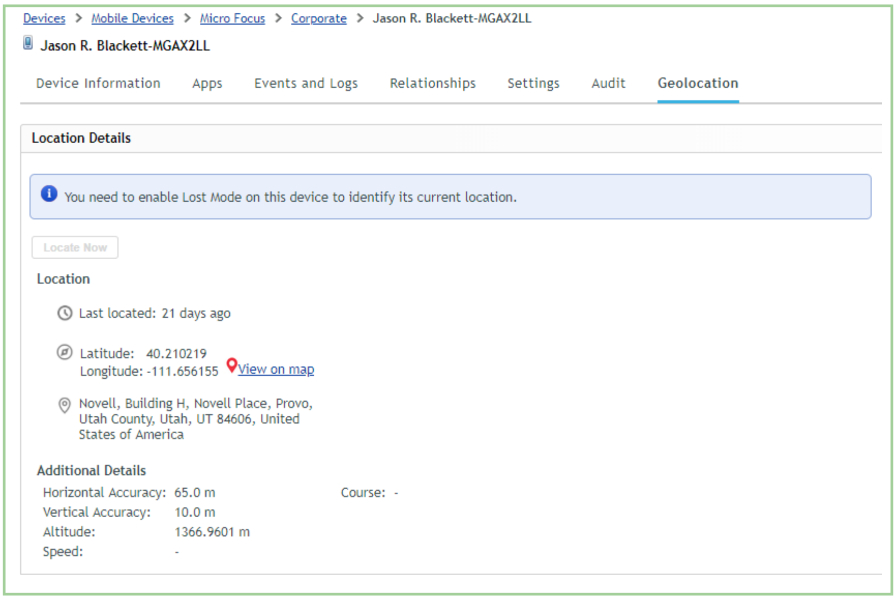


Figure 4: Geolocation of mobile devices

Mobile Management

If you are familiar with ZENworks 2017, then you know that we have been working on transforming ZENworks from a Client Management solution to a full Unified Endpoint Management solution. We continue this work in ZENworks 2017 Update 3, adding several key mobile capabilities.

iOS Lost Mode and Geolocation

ZENworks 2017 Update 3 provides support for locating an end user's lost device and, in the case of iOS, securing the device. The requirements for locating a device differ by platform, given the API set available on iOS or Android. For iOS, you can locate supervised devices by first triggering a quicktask to put the device into Lost Mode.

This restricts the device completely, preventing anyone from accessing it without first contacting the administrator. Once the device is in Lost Mode, you can then initiate a quicktask to find to the device from the new Geolocation tab on the mobile device, as shown in figure 4.

You can see that once a device is located, it displays the geolocation coordinates as well as the friendly place name and the accuracy data. From here, you can also click View on the map to open those coordinates on Google Maps and see the location.

On Android devices, there is no Lost Mode capability, but you can simply initiate a geolocation for any device that has the ZENworks app installed. Some Android devices require that the device be configured for high-accuracy mode for the location in order to be retrieved by the MDM agent.

Android Enterprise Work Managed Device Support

In ZENworks 2017 Update 2, we added support for BYO Android device management by supporting Work Profile enrolment. With the release of Update 3, we are bringing similar capabilities to corporate-owned devices by supporting Android Enterprise Work Managed Device mode. In the Android world, this is analogous to supervising an iOS device. Similar to iOS supervision, this is a destructive task— meaning that in order to manage the device as a Work Managed device, you must first factory-reset the device and then during factory-reset, provide a ZENworks-specific string that indicates the device will be managed by ZENworks.

This will cause the ZENworks application to be installed as the

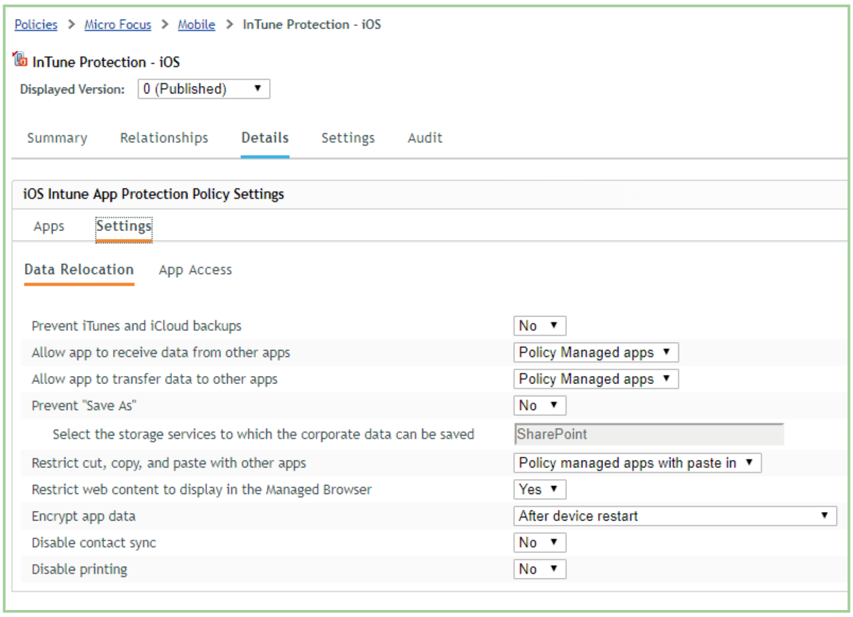


Figure 5: InTune application protection policies

trusted MDM solution on the device. Once installed, the end user can enrol with ZENworks in the same way as other devices.

With *Work Managed* mode, the end user will only have access to applications that the administrator grants and might not be able to add their own accounts to the device. In addition, any policies will impact the full device, unlike Work Profile mode where only access to the corporate profile is restricted.

InTune Application Protection Policies

Recently, Microsoft added support to the Graph API, enabling vendors to interact with the InTune Application Protection capabilities. These capabilities can be implemented to restrict the behaviour of Office 365 applications and other InTune, container-enabled applications.

With InTune Application Protection policies, you can do all of your mobile management from ZENworks and still have the benefits of being able to protect your sensitive Office 365 data. (Figure 5).

It is important to note that in ZENworks 2017 Update 3, InTune application protection policies have only been implemented for iOS; we will extend this to Android in the next update.

This decision was based on our experience with the Microsoft capabilities being substantially more stable on iOS than on Android at present. It is also important to note that in order to use these capabilities, the users you assign the policy to must have a valid InTune App Protection license assigned to them in Azure AD.

Also, unlike most policies in ZENworks, the InTune App Protection policy does not allow for the creation of a sandbox version for testing.

The reason for this is that when you are making changes to the policy, those changes are being written back to the Azure cloud, which currently does not provide any sandbox-like capability.

ZENworks does still maintain multiple versions of the InTune app protection policy so that you can revert to a previous version if required.

Other Enhancements

ZENworks 2017 Update 3 also provides the following notable enhancements:

- Configure the mobile inventory settings through ZCC
- Report on mobile inventory from ZENworks Reporting
- New iOS device control settings to prevent users from adding their own Wi-Fi and/or VPN configuration
- New iOS DEP settings supported in the latest version of iOS
- Reboot or shut down an iOS device remotely
- Send audit data and message data to syslog server for integration with SIEM solutions such as Micro Focus® ArcSight and Sentinel
- Automate the checking for and deployment of PRUs
- Improved recognition of Windows 10 versions and the ability to use that version information (1703, 1803, etc.) in system requirements and dynamic group filters
- Change the display size of the ZENworks User Application icons to provide an experience more consistent with the previous ZENworks Application Launcher
- Support for managing SLES 15 and OpenSUSE LEAP 42

Summary

ZENworks 2017 Update 3 is poised to be another great release that provides many capabilities to help further reduce the administrative overhead associated with managing your diverse endpoint estate and to improve your visibility into the system. We anticipate the release early in the second half of 2018.

We extend a big thank you to all our beta testers, engineers, and others who help us ensure a high-quality experience with each release!

Jason Blackett is the Product Line Manager for Endpoint Management at Micro Focus with a long history with ZENworks. His passions include cooking, his six children and ZENworks. He is based in Provo, Utah.

SecureData Sentry Simplifies Data-centric Security

Voltage SecureData Sentry is a significant new release and addition to the established Voltage SecureData product family. This addition to the SecureData portfolio is a data privacy broker that deploys easily into existing infrastructure. It transparently protects data fields and files flowing to or from the cloud, and in and out of applications and databases. The solution supports different content formats and protocols with a mix of protection mechanisms.

Fundamentally Voltage SecureData de-identifies data, rendering it useless to attackers, while maintaining its value for business processes, applications, and services. SecureData neutralises the impact of a data breach by making protected data worthless to an attacker.

SecureData Sentry simplifies and accelerates data-centric security deployment in cloud, commercial, and in-house applications without critical application changes or integration required. SecureData Sentry brokers data privacy to enable policy compliance on protected data.

The key benefits of Voltage SecureData Sentry are:

- Simplifies data protection for a wide range of applications without modification
- Accelerates time-to-value with flexible deployment of data security across hybrid IT
- Maintains centralized enterprise control over encryption keys and data in cloud services
- Promotes a non-disruptive, transparent approach to privacy compliance and the secure use of data
- Enables interoperability of encrypted data between multiple SaaS applications, independent of company size or geography

Today´s data-driven enterprises face dissolving organizational boundaries and the adoption of cloud applications ensures data is constantly flowing to and from on-premises systems and cloud services. This includes SaaS applications, commercial off-the-shelf (COTS) applications, and in-house applications.

Strict privacy regulations, such as GDPR, PCI DSS, and HIPAA along with limited trust in hosted environments, make the protection of personal data imperative, anywhere such data may exist. The availability of Format-Preserving Hash, the newest innovation in Voltage data protection methods, provides non-reversible de-identification, supporting use cases which call for data anonymisation.

Sentry leverages proxy interception and API technologies to support a broad variety of SaaS applications, such as Salesforce, ServiceNow, ALM Octane, Microsoft Dynamics 365, and others. The solution accesses and protects sensitive data flowing through the network, ensuring organizations remain in control of data used in cloud applications.

The same technology can be used to secure COTS and in-house applications, providing an alternative to API integration that avoids the need for programming. SecureData Sentry's inspection, or "discovery" mode, identifies the data fields in your target applications, allowing easy configuration of field-level protection.

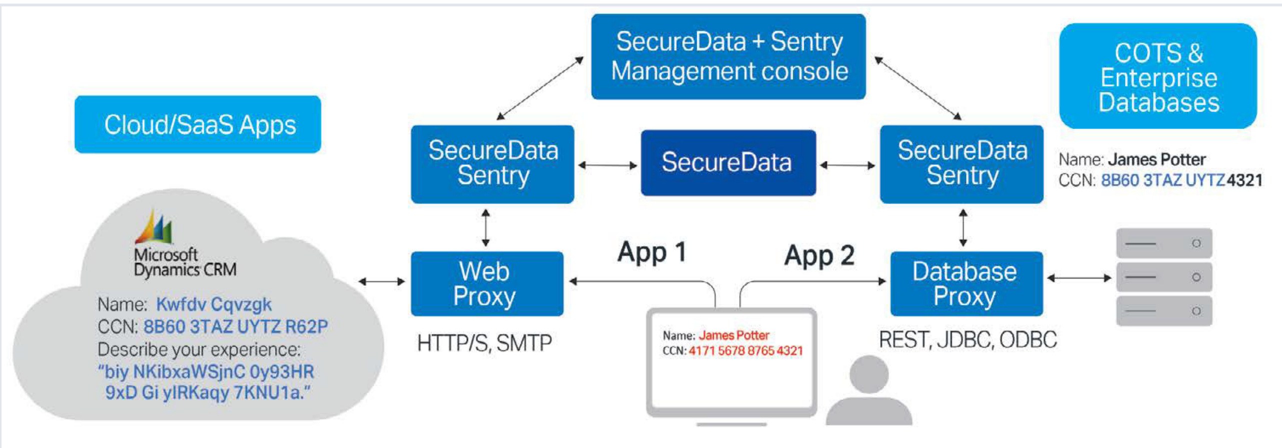


Figure 1: A typical scenario for SecureData Sentry

Format	Example 1: Data Element	Example 2: Data Record
Original Data	Tax ID: 934-72-2356	First name: Gunther Last name: Robertson SSN: 934-72-2356 DOB: 08-07-1966
FPE AES-FF1 mode	253-67-2356	First name: Uywjlqo Last name: Muwruwwbp SSN: 253-67-2356 DOB: 08-07-1966
Regular AES-CBC mode	8juYE%Uks&dDFa2345^WFLERG	Ija&3k24kQotugDF2390^320OWioNu2(*872weW Oiuqwriuweuwr%oIUOw1@

Figure 2: Examples of Format Preserving Encryption (FPE)

SecureData Sentry centralises management on-premises, enabling organizations to retain authority over their own cryptographic keys and token tables, and simplifies security deployment. SecureData Sentry accesses data streamed over key communication protocols, including HTTPS and SMTP, and through popular APIs, including REST, SOAP, JDBC, and (very soon) ODBC.

SecureData Sentry simplifies deployment and extends the reach of Voltage market-leading data protection technologies, including Hyper Format-Preserving Encryption (FPE), Hyper Secure Stateless Tokenization (SST), Stateless Key Management, and Format-Preserving Hash (FPH). Leveraging the NIST FF1 AES encryption standard, Voltage SecureData is unique in being the only FPE product to be Common Criteria certified, and FIPS 140-2 validated.

Hyper FPE - encryption and masking – is a highly effective method of preserving data security. Traditional encryption approaches, such as AES CBC, have enormous impact on data structures, schemas and applications. Hyper FPE is NIST-standard using FF1 mode of the Advanced Encryption Standard (AES) algorithm, which encrypts sensitive data while preserving its original format without sacrificing encryption strength. Structured data, such as Social Security number, Tax ID number, credit card, account, date of birth, salary fields, or email addresses can be encrypted in place. Figure 2 provides simple examples.

Like traditional AES, the Hyper FPE algorithm uses strong 256 bit keys, and like AES, with the ciphertext and the original key, an application can get back the unencrypted value. A variation of this technology allows the identity and access policy data to be embedded within the cipher text.

Traditional encryption methods significantly alter the original format of data. For example, a 16-digit credit card number encrypted with AES produces a long alphanumeric string. As a result, database schema changes are required to facilitate this incompatible format. Hyper FPE maintains the format of the data being encrypted so no database schema changes and minimal application changes are required—in many cases only the trusted applications that need to see the clear data need a single line of code.

Another aspect that is key for the deployment of innovations such as Big Data, cloud and Internet of Things is performance. Hyper FPE allows accelerated encryption performance aligning to the high volume needs of next generation business initiatives. Tools for bulk encryption facilitate rapid de-identification of large amounts of sensitive data in files and databases. Also whole systems can be rapidly protected in just days at a significantly reduced cost.

SecureData Sentry is comprised of the following components:

- Management Console - role based administration interface to manage Sentry, fully audit enabled.
- Server - a software appliance to manage protection (keys) to files and fields, scalable with HA and load-balancing options. High performance; supports forward and reverse proxies, and database drivers.
- Privacy Services for Databases - services to protect data in databases, supporting ODBC and JDBC, as well as APIs for NoSQL databases.
- Protection Mechanisms - Methods that support Voltage Hyper FPE, SST, FPH, static and dynamic data masking, and stateless key management, with all different content formats.

Further information can be found at microfocus.com/media/data-sheet/voltage_securedata_sentry_ds.pdf but the Voltage SecureData product range will be fully explored in future articles.

Succeeding In The Journey To Agile And DevOps

Quality delivery with the Micro Focus® Application Lifecycle Management (ALM) solution

Agile and DevOps are clearly here to stay. The majority of today's enterprises are gradually adopting Agile practices for application development, and many are transitioning to DevOps. But while these two approaches rapidly gain momentum, many organisations continue to support traditional Waterfall processes and tools. The reality is that most rely on a mix of different methodologies, technologies, and processes. Regardless of the development approach and processes in use, development teams have one important goal in common: achieving faster time-to-market without compromising quality.

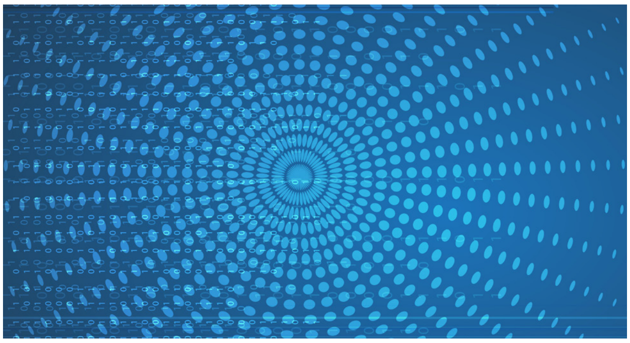
Dealing with Challenges in the Journey

Without question, there are many challenges on your way toward Agile and DevOps. One of the most significant is coordinating the work of several development teams with multiple management methodologies. Some Agile project management tools work well for individual teams but don't facilitate cross-team visibility and collaboration.

In addition, adopting Agile practices at enterprise scale is not easy. It is a journey with no defined path—requiring incremental steps—and you'll need to discover the precise path that fits your needs. During the process, you will typically rely on a mix of Waterfall and Agile processes and tools. This means you need a flexible lifecycle management solution that adapts to your needs as your teams grow in maturity and scale. Otherwise, you may suffer high maintenance costs and low productivity due to the use of several disparate and disconnected tools.

As you move forward in adopting Agile, your processes will likely expand to accommodate quality assurance (QA). In doing so, you may face challenges when a lack of automated tests results in more work and late discovery of issues. When you are ready to further extend Agile practices to your operations team, traditional processes might be jeopardised due to the increased speed of deployment. How does your team meet uptime and availability SLAs with so many frequent releases into production? The bottom line is that once something needs to be fixed, if you don't have traceability across the DevOps landscape you can't resolve issues with the required speed.

Micro Focus helps you solve these challenges with our Application Lifecycle Management (ALM) solution, which includes ALM/Quality Center and ALM Octane. For many years, Micro Focus ALM/Quality Center has served a large and growing customer base, including all of the top 25 Fortune 500 companies. Micro Focus ALM Octane extends the proven capabilities of ALM/Quality Center and is built specifically with Agile and DevOps in mind.



Succeeding in the Journey—Typical Scenarios

Transitioning to Agile and DevOps is a journey that can't be accomplished overnight. The Micro Focus ALM solution provides the support you need at each step along the way.

Following are five typical scenarios that illustrate the journey from traditional Waterfall development to Agile and DevOps. Through these examples, you can see the specific advantages that Micro Focus ALM/Quality Center and ALM Octane offer to your development and testing teams.

The scenarios include:

1. Using traditional Waterfall
2. Starting small with Agile
3. Using a hybrid approach
4. Scaling Agile
5. Moving from test automation to DevOps

1. Using Traditional Waterfall

Although "pure Waterfall" development environments are less and less common, many organisations still have a mix of Waterfall and Agile projects. In highly regulated industries and large non-software projects, Waterfall still has its place.

Traditional Waterfall methodology is project-based: you define a set of requirements at the beginning, specifying what the business wants, and a timeframe for delivery. The challenge in Waterfall is that later changes to requirements greatly impact the project in terms of time, money, and quality. This means change management is critical. ALM/Quality Center has rich features to support these efforts, such as baselining, version control of requirements, change-impact reporting, and risk-based quality management.

ALM/Quality Center also provides many best practices templates for managing and tracking Waterfall development, designed to help you increase the success rate of your projects. Traceability to test results and defects keeps project managers and QA managers aware of the realtime status of project quality, so that they can make the right decisions.

2. Starting Small with Agile

The most successful introduction of Agile usually starts small. If you are currently using ALM/Quality Center to develop applications with Waterfall, often the best approach is to introduce Agile by enabling a few teams to start using ALM Octane.*

Micro Focus provides seamless synchronisation between ALM/Quality Center and ALM Octane, so that you can continue to monitor and manage a total view of all projects using ALM/Quality Center.

Some organisations use a Project and Portfolio Management (PPM) tool to manage Waterfall and Agile projects together. If you are already using Micro Focus PPM, you can easily upgrade to gain the ability to centrally manage hybrid projects.

3. Using a Hybrid Approach

Once you have proven the value of Agile through successful implementation for a small number of teams, you may decide to extend the practice to more projects. But some types of projects are more difficult to transition to full Agile immediately. That's why there are several hybrid approaches. You may decide to use a mixture of methodologies in a single project or employ a combination of management tools.

Following are two typical hybrid use cases. After reviewing these, you can evaluate your own specific situation and decide whether to manage your hybrid projects using ALM Octane alone or ALM/Quality Center and ALM Octane together.

- Hybrid Development using ALM/Quality Center and ALM Octane

If you are currently using ALM/Quality Center, you can easily do hybrid development with ALM Octane added. The close integration between the two tools allows you to be flexible in the pace and path of Agile adoption. You can create a project in both ALM/Quality Center and ALM Octane and synchronise data between them, and can gain a consolidated project view from either tool.

In this scenario, you can continue to take full advantage of the ALM/Quality Center features your business relies on while increasing the span of Agile adoption step by step.

Using ALM Octane for Agile management provides user-friendly backlog management and sprint management functions, as well as a rich set of Agile reporting widgets such as Sprint burndown, Sprint velocity, Epic burnup, and Velocity planned vs. Actual. The Team Backlog module gives each team its own space, and the Quality module provides QA teams with a view of the quality of each application component, so that issues of one component can be addressed without dependency on others.

Test automation and continuous integration become mandatory at this stage. Without these features, you can't get feedback early and truly enjoy the benefits of Agile. ALM Octane is your choice for this purpose. You don't need another tool—instead, take advantage of the ALM Octane test and quality management capabilities.

- Consolidating Hybrid Development Management into ALM Octane

If you are using multiple tools to manage your traditional and Agile projects separately, the effort and cost to maintain the system can be greatly reduced by moving to a single tool—ALM Octane. In addition, the ALM Octane client is pure HTML5 web-based, so that when there is an upgrade, you don't need to do anything at the client side. This also gives you more flexibility in the devices and browsers you choose to use.

You may have already introduced tools like JIRA to your Agile teams, and if so, you may be struggling with lack of traceability and cross-project visibility. ALM Octane provides a working synchroniser with JIRA, as well as cross-project reporting capabilities. Migrating to ALM

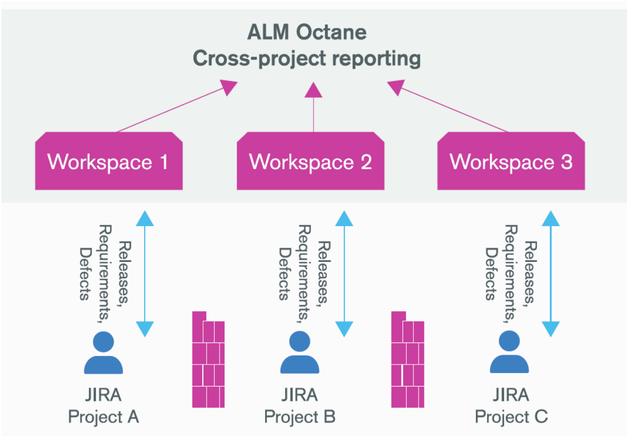


Figure 1: ALM Octane brings perspective across JIRA teams

Octane reduces your need for additional, specialised tools—thus decreasing your TCO. As a result, you not only reduce cost but also gain the traceability you didn't have before.

Requirements, code, builds, tests, deployments, and defects are all inter-linked—enabling a true lifecycle view of your projects. In addition, you have access to an overview that shows what is going on in the delivery pipeline. You will see where a code change is—whether it is failing at build, has become a release candidate, or is somewhere in between. This is very crucial in assuring quality when the pace of development becomes faster and faster.

4. Scaling Agile

When hybrid Agile practices succeed and you achieve a sustainable speed of delivery, you may want to scale projects and teams to a larger scope. To address the challenges of scaling, several enterprise Agile scaling frameworks have emerged, such as SAFe (Scale Agile Framework), LeSS (Large-scale Scrum), Nexus, DAD (Disciplined Agile Delivery), and Spotify. ALM Octane serves you well when you adopt any of these frameworks.

ALM Octane is built with SAFe support in mind. Its entity structure follows the SAFe concepts of Epic, Feature, and Story, and it has all the features to implement SAFe up to program level. By integrating with Micro Focus PPM, all configurations of SAFe can be implemented.

ALM Octane also provides the mechanism for you to implement DAD. DAD emphasises a goal-driven approach as opposed to prescriptive methodologies. ALM Octane is highly flexible, enabling you to customise it to support any methodology suitable for your specific situation.

Common to all scaling frameworks is the need to support a large organisation with multiple products and multiple teams. ALM Octane is designed for such scenarios. The cross-workspace customisation and reporting it provides are very important in implementing any scaling frameworks.

In addition, most large enterprise Agile frameworks recognise the importance of governance and enterprise awareness. ALM Octane provides workflow, template, DevOps governance, and strong security features for organisations adopting these frameworks.

5. Moving from Test Automation to DevOps

Some Agile management products support only planning and tracking and require another tool for test and quality management. ALM Octane provides planning, tracking, test, and QA features in a single tool. Wherever you are in Agile transformation, ALM Octane provides valuable capabilities including test automation, reporting, quality management, failure analysis, and the ability to eventually transition to DevOp.

Even before Agile became popular, test automation was the goal of many software development teams. That's why Micro Focus Unified Functional Testing (UFT) was created and has been very well received by our customers. ALM/Quality Center has a set of features to manage and execute UFT tests effectively and track test results.

However, the automation achieved was within specific scope, not end-to-end. In recent years, the advent of some open-source and non open-source tools finally made end-to-end automated test the reality. Today it's no surprise that even Waterfall projects use Jenkins for build and test execution.

When you want to extend Agile to QA, a tough obstacle to tackle is to automate all tests, including unit tests, integration tests, user acceptance tests, performance tests, and so on. Provisioning of the test environment needs to be automated as well. In response to this challenge, ALM Octane puts a tool chain in your hands.

Tools for all sorts of test and verification can be added to the chain to build complete automation. Integrating Micro Focus Service Virtualization into the tool chain brings significant savings in testing time by removing test restrictions caused by delays in availability of external services and software components. You can also execute UFT tests in the tool chain.

ALM Octane presents a new way of creating automated tests, with its built-in BDD framework backed by the Gherkin test mechanism. It allows you to turn manual tests into auto-tests very easily, using Cucumber or SpecFlow. This is one of the most attractive features embraced by customers who have adopted ALM Octane.

DevOps

After Agile is fully part of your development processes and QA is successful, you can begin to think about extending it to operations. This can be a much bigger challenge than the previous steps. To meet availability and other SLAs, Operations teams don't like frequent changes in the production environment. They are right: frequent releases, without a high confidence in quality, can put your business in danger.

DevOps is meant to solve the dilemma. It enables you to build a vehicle to automate and accelerate the development and operations processes. Starting with continuous integration, ALM Octane lets you extend the range of full automation to the entire application lifecycle.

ALM Octane integrates with leading continuous integration server products such as Jenkins, TeamCity, and Bamboo. You can integrate a wide range of source-control management tools, testing tools, and others. More importantly, the traceability from requirements/defects to the relevant code changes, builds, and tests is established in ALM Octane. Based on this traceability, ALM Octane can identify hotspots and risky commits in your code, to let you proactively take caution. Traceability can drastically speed up the resolution of production issues.

ALM Octane manages the large number of pipelines needed by enterprise-level development. It visualises the topology of each pipeline, as well as the build status and trends. In addition, build failures can be broken down to application-component level. The failure analysis feature has the intelligence to categorise failure reasons, identify test failure patterns, and find the developers potentially related to the failure. ALM Octane also integrates with release automation tools such as Xebia XL, to let you enforce the criteria to meet before the final release decision. With everything automated in the pipeline, it will seem as if your applications are created in an assembly line with predictable high quality.

Key Takeaways

- Start your Agile and DevOps transformation with ALM Octane to avoid disconnection between Agile teams or Agile vs. Waterfall silos from the very beginning.
- Reduce TCO by consolidating separate tools into ALM Octane.
- Use ALM Octane to modernise your test and quality management, achieve end-to-end automation, and extend Agile practices to QA and Operations
- ALM Octane adapts to your needs as your organization grows in Agile/DevOps maturity and scale, and achieves higher return on investment.

About Micro Focus ALM/Quality Center

ALM/Quality Center is a highly functional industry-leading application lifecycle management platform. Highly customisable and scalable, it can meet many different enterprise business needs.

ALM/Quality Center provides strong support to Waterfall projects and projects that have regulatory compliance needs. ALM/Quality Center also addresses the need for a stronger connection between business process modelling, quality management, and requirements definition. In addition, it manages tests created with the business process testing framework, allowing you to reuse the test components based on business processes to increase test flow ROI.

About Micro Focus ALM Octane

ALM Octane—the application lifecycle management tool built precisely for enterprise-level Agile and DevOps—offers a full set of Agile management features but is methodology-agnostic, supporting any methodology or a mix. Its innovative DevOps features enable your development teams to embrace leading open-source and non open-source technologies, which can significantly accelerate their work.

The test and quality management features built into ALM Octane bring better end-to-end traceability—with insights into source code, build, and the entire DevOps pipeline. ALM Octane provides a single view of the truth across the entire development and test environment. The Behavior Driven Development (BDD) framework is highly valued by our customers because it enables them to turn manual tests into auto-tests very easily. Like ALM/Quality Center, ALM Octane is highly customisable and scalable.

Why Micro Focus for ALM?

Micro Focus is a global software company with 40 years of experience in delivering and supporting enterprise software solutions that help customers innovate faster with lower risk. With more than 6,000 large-enterprise customers worldwide, Micro Focus is a proven leader in lifecycle management solutions. Our mission is to support our customers' application development environments regardless of the methodologies and processes they are using.

Learn More At

1. *https://software.microfocus.com/en-us/products/application-lifecycle-management/overview*
2. *https://software.microfocus.com/en-us/software/alm-octane*

Success Story: Monte Dei Paschi Di Siena

Monte dei Paschi di Siena (MPS) is one of Italy's largest banks. Formed in 1472, it is also the world's oldest. Today, the business has around 2,100 branches and 30,000 employees. To remain competitive, Monte dei Paschi di Siena needed to reduce IT costs and optimise performance while providing IT services that improve the business. To accomplish these goals, the bank turned to Micro Focus Enterprise DevOps software.

Creating efficiencies through better testing

Its size and age have not prevented MPS from being impacted by wider challenges in the financial sector. "We are working hard to reduce IT costs and optimise our performance," says Michele Rizzo, IT development architecture and IT automation manager, MPS. "From a business point of view this means smarter banking—promoting online and mobile banking, all of which requires a stronger, more efficient IT. We need to be better at providing the IT services the business can use."

Ultimately, Rizzo continues, it is about having a clearer focus on the customer: "We need to identify what the customer wants, and deliver those services quickly and faultlessly." From an IT point of view this means detecting incidents early and resolving them quickly.

Strong IT governance is key to IT stability, Rizzo continues: "We wanted to create a methodology to support release management and standardise our development environments. This would increase the quality and efficiency of our software development, and reduce the number of defects."

"We are very keen to be self-sufficient in terms of managing and maximising the use of our software

MONTE DEI PASCHI DI SIENA
BANCA DAL 1472

tools, though we know we can lean on HPE Software Services (now part of Micro Focus) for help with special projects."

Strength through testing

MPS was already a user of Micro Focus Project and Portfolio Management (PPM). "HPE PPM (now part of Micro Focus) has delivered speed and quality improvements," says Rizzo.

The next step in the bank's journey to DevOps was to adopt the suite of Micro Focus Application Lifecycle Management (ALM) tools, from change and release management, to configuration management, to release automation. The final phase would be a full Enterprise DevOps integration, bringing together people, processes, and technology.

This would drive efficiencies, particularly from the people and process perspective, improving cross-functional collaboration between testing and development. This Enterprise DevOps initiative would enable MPS to proactively reduce the number of defects and consequently drive production efficiencies.

"My perception is that Micro Focus, particularly in regard to testing and integration, is probably one of the best three suppliers in the world of this kind of solution," says Rizzo. "It has 30 years of expertise in this field." Micro Focus Software Support services worked hand-in-hand with MPS to develop a DevOps solution that not only integrated seamlessly with its current business processes, but enabled MPS to understand the DevOps solution, with a view to achieving long-term self-sufficiency.

This DevOps journey encompassed two phases: testing standardization and release management, followed by configuration and deployment management. Software Support services would be on hand during the pilot phase, including running a special management-of-change project to fully engage MPS stakeholders, with a view to the bank being self-sufficient at roll-out.

"We were conscious this deployment had to be more than simply the right tool, we needed the implementation to fit with our processes. HPE Software Services would ensure the technology worked best with our people and processes, but it would

"We wanted a solution that was as 'out-of-the-box' as possible, or customised as little as possible…We have the solution we wanted."

MICHELE RIZZO
Manager, IT Development Architecture & IT Automation
Monte dei Paschi di Siena

At a Glance

Industry:
Financial Services

Location:
Siena, Italy

Challenge:
Monte dei Paschi di Siena needed to provide better IT services so that it could increase cross-functional collaboration to improve the quality and effectiveness of business efficiency.

Solution:
The bank created a new approach to IT services using a solution that is based on Micro Focus Enterprise DevOps.

Results:
+ Increases efficiency and quality of software development
+ Creates a consistent testing practice with minimal complexity, simplifying future upgrades
+ Builds a stronger bank through better testing
+ Allows faster delivery of new IT services to the business, strengthening competitiveness in a tough market

also allow us to watch and learn, and maybe adjust our processes to work more efficiently," explains Rizzo.

"We are very keen to be self-sufficient in terms of managing and maximizing the use of our software tools, though we know we can lean on HPE Software Services for help with special projects."

A committed partner

Only part-way through the pilot phase, Rizzo says it is too early to assess the business impact of the bank's DevOps solution—specifically, whether it will help halve the number of defects while increasing operational efficiencies—but he is confident that Enterprise DevOps has set a good foundation on which MPS can build: "We're still at the pilot stage, testing on just two out of 600 applications. But it is clear we are in a better position from an IT cost and quality perspective— and that can only benefit the business. Right now, we're confident we can expand."

Rizzo says the involvement of Software Support has been instrumental in creating an effective DevOps solution. "We have established an excellent working relationship. We have a steering committee involving the bank's IT senior management, with HPE sat alongside. It is more than a client-supplier relationship; it is a partnership. We were both committed to the success of the project."

Software Support services, he continues, never lost sight of the bank's requirements: "We wanted a solution that was as 'out-of-the-box' as possible, or customised as little as possible. Of course, it needed to be tailored to our process, but complexity can be dangerous, especially when you want to move to the next release. We have the solution we wanted."

Using the insight and expertise of Software Support services, IT management is now focused on developing DevOps competencies within its own organisation as it begins a self-sufficient roll-out of Enterprise DevOps across its application landscape. Software Support services will continue to provide support for special projects and the MPS competence center. The future, Rizzo says, is to expand the Enterprise DevOps solution to all IT systems within the business, improving the quality of software and service supplied to the business.

"The better the service we can provide to the business," he says, "the better the business."

Learn More At
1. microfocus.com/solutions/enterprise-devops
2. software.microfocus.com/en-us/software/alm-consulting-services

Micro Focus Release ESM 7.0

ArcSight Enterprise Security Manager (ESM) 7.0 is the latest release of the market-leading solution that prioritises security threats and compliance violations with real-time threat intelligence to quickly identify and impede potential cyber-attacks. By collecting, correlating, and reporting security event information at a massive scale, Micro Focus ArcSight ESM 7.0 helps organisations meet even the most demanding security requirements, while simplifying and improving time to value.

The big new feature is **distributed correlation.** ESM 7.0 combines the most powerful SIEM correlation engine with distributed node/cluster technology. By decoupling the components used in the advanced correlation processes, customers can now add additional nodes to the ESM cluster, scaling ESM like never before, analysing up to 100,000 events per second.

The sheer amount of data that Security Operations Centers (SOCs) have to deal with can be overwhelming. Sifting through the noise, prioritizing analysis and response efforts and confidently using threat intelligence to make the right decisions is extremely difficult. Furthermore, the only way to extract intelligence from the data is through a central processing unit (CPU) and memory intensive analytics and correlation.

With distributed correlation, Micro Focus offers a powerful, new way to scale SIEMs analytics and event correlation without the need to incur excess costs, so that customers can focus on providing security insights and scaling their business without limits.

ArcSight ESM will be reviewed in full in forthcoming issues of OH Magazine, but you can learn more now at https://software.microfocus.com/en-us/products/siem-security-information-event-management/overview

File Dynamics: Addresses The Expanding Requirements Of Data Management

by Buck Gashler

"Data really powers everything we do".[1] It has been called the "raw material[2]" of business. That is why proper data management is so important. However, the term "data management" is one that is continuously evolving. Today, a variety of factors including the overwhelming growth of data, compliance to data-specific industry and government regulations, and the increasing incidents and sophistication of ransomware are causing organisations to make data management a bigger focus of their activities.

This greater emphasis on data management, along with its continued evolution, is the catalyst for the expanded data management services offered by Micro Focus in a new product released in May – File Dynamics 6.0. At this point, one might logically ask why a brand new product offering is being introduced as version 6.0.

Well, at the core of File Dynamics are the legacy identity-based file system management capabilities of Micro Focus Storage Manager for Active Directory (a product that is still available for purchase). File Dynamics was engineered from this legacy system, but then greatly expanded the policy-based management capabilities from merely Identity-Driven policies, to now Target-Driven policies.

Product Overview

File Dynamics provides extensive services to address the expanding requirements of network data management. Identity-Driven policies automate tasks that are traditionally done manually, resulting in cost savings and assurance that tasks are being performed properly. Target-driven policies offer data migration, remediation, cleanup, and protection from data corruption and downtime through nearline storage backup of vital data, referred to as "High-Value Targets," enabling quick recovery of files and their associated permissions.

> ***Editor's Note:*** *This article is an update to the same titled article that was published in OHM39, p14-17, 2017/4. As the product's originally planned January release date was rescheduled to May so that Workload policies could be introduced in the product, we are publishing this updated version.*

Data Management Delegated to Data Owners

An important aspect of File Dynamics is the introduction of "Data Owners" and their role in performing limited, but important data management tasks. A Data Owner is a user specified in a File Dynamics Target-Driven policy who is enabled to perform data recovery and remediation tasks, based on the user's designation as a Data Owner, and the user's familiarity with the data.

For example, compared to a regular IT staff member, an employee in the Legal Department of an organization is much more knowledgeable about the files and folders being stored and accessed by the Legal Department employees. Therefore, it makes sense for an administrator to designate a user in the Legal Department to be a Data Owner for that department.

Data Owners are enabled to recover data and remediate the location of sensitive files to more secure locations.

Identity-Driven Policies

Identity-Driven policies affect user and group objects that make up the Microsoft network operating system's directory service – Active Directory. A User Home Folder policy or a Group Collaborative policy specify the settings for managing network storage areas for user and group objects respectively in Active Directory. For example, you could create a User Home Folder policy that was associated with the Human Resources organisational unit of your Active Directory forest. The settings within that policy would then apply to all user objects that reside in that organisational unit.

The settings within an Identity-Driven policy specify how user and group data is automatically provisioned, how common management tasks are automatically conducted, and how it is automatically cleaned up.

We covered the Identity-Driven features in a previous article on Storage Manager (OHM35, 2016/4, p26-28), so the focus here will be on the new Target-Driven policies.

Target-Driven Policies

Through Target-Driven policies, File Dynamics performs management tasks through policies associated directly with a network share of a folder. Target-Driven policies include Data Location policies, Content Control policies, Workload policies, and Epoch Data Protection policies.

Data Location Policies policies are the means of copying folders and their contents to a target parent folder. There is an option to remove the files from the source location after they have been copied. For example, if you were performing a server consolidation or moving data from a server to a NAS device (or vice versa), you could do so easily using Data Location policies.

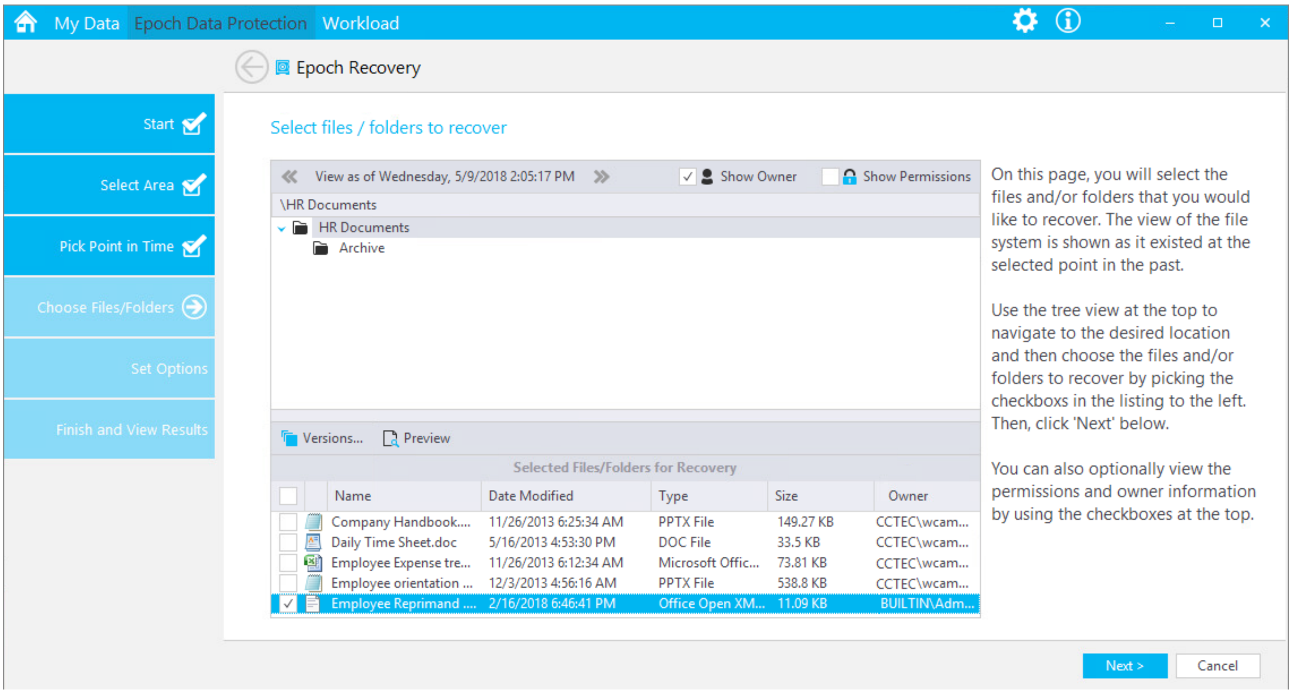


Figure 1: In this example, a Data Owner is using a wizard to specify files for recovery.

Content Control Policies. Similar to Identity-Driven file grooming, Content Control policies remove files according to file type, age, size, when last accessed, and more. From any file path, you can either vault files to a new location or delete the files altogether. You could use this feature for example, to easily delete temporary files and in the process, make much more disk space available on your storage devices.

Workload Policies in File Dynamics provide the ability to handle work processes initiated from other applications. For example, reports generated in Micro Focus File Reporter that specify the locations of files containing credit card or U.S. Social Security numbers (a new capability introduced in File Reporter 3.5) can be imported into the Data Owner Client where a designated Data Owner can remediate the location of these sensitive files from an open share, to a more secure location. This approach empowers organisations to provide automated network file system security remediation approved by a gatekeeper familiar with the files.

Epoch Data Protection Policies. As organisations have had to deal with the increasingly devastating effects of ransomware, they are looking to solutions that provide data continuity. Data continuity is a term that includes the measures taken to safeguard the integrity and availability of critical data so that when an event takes place that either corrupts the data or disables access to it, restorative remediation can take place quickly and with minimal disruption.

Logically, one might conclude that the organisation's backup system would take care of this, but the sophistication of recent ransomware attacks has many security experts recommending that you keep multiple backups[3] in various locations, with restrictive administrative and system access.[4]

Moreover, restoring data from traditional backup systems can be time consuming as it oftentimes requires IT administrators to sort through the contents of an entire system backup.

In addition to safeguarding against ransomware attacks, there are other reasons why an organisation would want to protect data through additional data continuity measures. These include:

- Protecting data from inadvertent corruption, loss, or deletion
- Restoring the data back to how it existed at a particular point in time in the past

Similarly, organisations might need to protect and recover the permissions of High-Value Targets, including:

- Lost or destroyed permissions
- Inadvertently changed permissions
- Permissions as they previously existed at a particular point in time in the past

Epoch Data Protection policies allow customers to maintain nearline standby views of High-Value Target folders stored in the network file system. Data Owners can view and access the archive of the High-Value Target as it existed at a selected point in the past. In essence, it is a "time machine" for the data and associated permissions on the High-Value targets.

Archived files are located in a "Collection" of "Epochs." An Epoch consists of the directory structure and associated metadata at a point in time. The Collection is stored in a nearline repository called a "File

Micro Focus File Dynamics Data Management and Protection

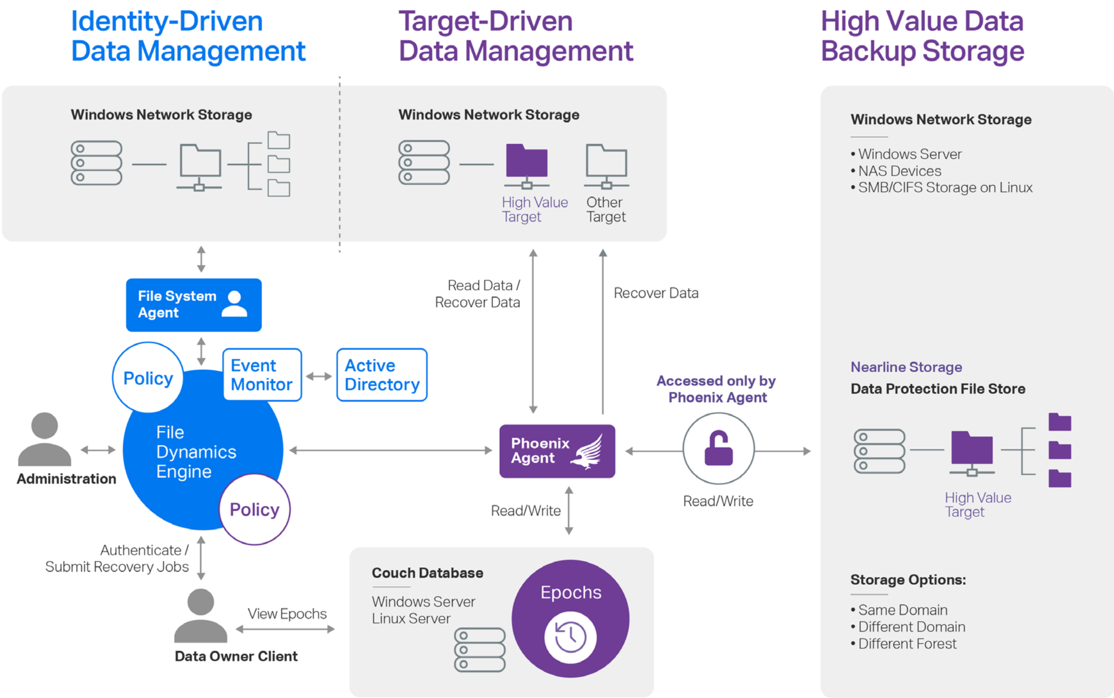


Figure 2: The File Dynamics Engine, in cooperation with the Agents enact the Identity-Driven and Target-Driven policy actions.

Store." Epochs are saved to the File Store through a proxy with no direct user access to the Collection. This creates a confined repository on the network that cannot be compromised by a user.

Recovering a file from the File Store is a multi-step process. Using the Data Owner client, the Data Owner first opens an Epoch and can then see the contents of the Epoch, with even the option of opening a "View" of an individual file.

The View is not the actual file, but a complete rendering of the file. Upon determining which files to recover, the Data Owner then makes a recovery request for those files.

The Data Owner Client authenticates to the Engine and the Engine then delegates the recovery to the Phoenix Agent, which recovers the files to either the location where the file existed previously or to a location of the Data Owner's choosing.

Unique Benefits

When it comes to data continuity, the Epoch Data Protection (EPD) offered in File Dynamics offers many enhancements in addition to vital backup systems.

1. The EPD interface is easy to use and administer. Using either a wizard or a console, you can locate a file you want to recover. Locating and selecting files is similar to locating files in the Windows Explorer interface. Administrators who have had to work with the complex user interfaces of other backup systems will find the EPD interface very intuitive.
2. With File Dynamics you can designate specific Data Owners to be in charge of restoring data and permissions from High-Value Targets. This offloads the responsibility from the overworked IT staff and in the process, enables a faster response and restoration time from the Data Owner—a critical factory in effective data continuity.
3. EPD uses limited read/write access to backup locations—a remedy for diminishing the threat of ransomware. With restricted network access to the protected High-Value Targets, data and their permissions remains protected from ransomware and other malware threats.
4. EPD lets you back up High-Value Targets as frequently as you would like and permits the Data Owners to verify the integrity of the backups. According to the Software Engineering Institute at Carnegie Mellon University, "The single most effective deterrent to ransomware is to regularly back up and then verify your system."[5]
5. The EPD repository is one more repository for your critical data. Security analysts recommend a multi-tier approach to provide more reliability with backups.[6]
6. EPD policies archive files quickly. That is because only files that have been modified since the last saved Epoch are backed up. However, when you open the

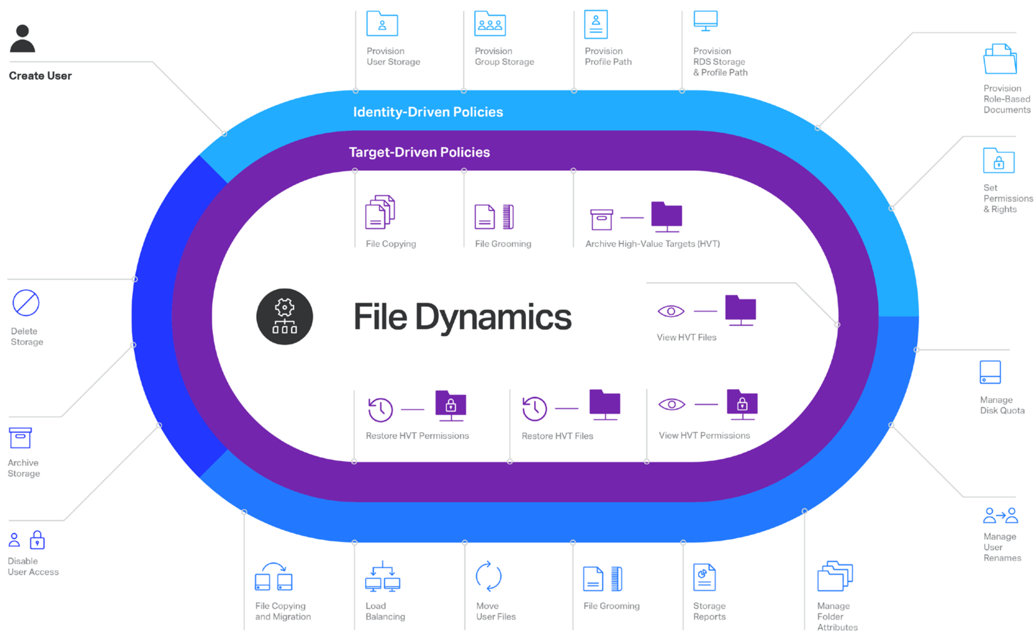


Figure 3: Summary of all data management capabilities that come from through Identity-Driven and Target-Driven policies.

new (or any) Epoch, it will contain *all* of the archived files in the High-Value Target – not just the modified files.

7. As you locate a file for recovery, you can view a complete rendering of the file to verify that the selected file is indeed the file you want to recover.

Expanding Data Management Services

Data management requirements have changed dramatically since we introduced our first data management product—File System Factory in 2003. Back then, the principle focus of the product was completing the account automation chain of identity management systems by automating the provisioning of network user storage locations in synchronization with the automated account provisioning provided by the identity management system. The product became an instant success—especially within organisations with a large number of user accounts.

Over time, the product name was changed to Storage Manager as capabilities were expanded to include features to solve other data management challenges—challenges that included addressing data growth, security, compliance requirements, data loss prevention, and more. As data management continues to evolve and its requirements continue to expand, Micro Focus is committed to continue to address those challenges.

With Identity-Driven policies providing automated user and collaborative data management, combined with Target-Driven policies that provide selected storage management and data protection, you have a data management system in File Dynamics that meets an extensive set of today's data management challenges.

As data management requirements continue to evolve, so will File Dynamics. Development plans are now in place for even more Target-Driven management capabilities that will be introduced in future releases.

Conclusion

Identity- and Target-Driven policies in File Dynamics together work to manage an extensive set of data management tasks that will save you money, help meet your compliance objectives, provide assurance that management tasks are being performed correctly, and provide you confidence that files located on High-Value Targets are being backed up and can be recovered quickly.

As network-stored data continues to grow, as regulations for data storage access and privacy continue to become more stringent and complex, and as threats from malware continue to wreak more and more devastation, the data management capabilities of File Dynamics are needed more than ever.

References

1. Jeff Weiner, CEO, LinkedIn
2. Craig Mundie, Senior Advisor to the CEO, Microsoft
3. Will your backups protect you against ransomeware?, Maria Korolov, CSO Online, May 31, 2016
4. Ransomware Damage Report: 2017 Edition, Herjavec Group, May 24, 2017
5. Ransomware: Best Practices for Prevention and Response, Alexander Volynkin, Jose Morales, Angela Horneman, May 31, 2017
6. Will your backups protect you against ransomeware?, Maria Korolov, CSO Online, May 31, 2016

Buck Gashler is the Marketing Director of Condrey Corporation which develops the Storage Manager and File Reporter components of the Micro Focus File Management Suite.

OES Means Business: Dispelling The Top 10 Myths

by Lothar Wegner

Open Enterprise Server 2018 delivers robust networking, file, and print services for your enterprise on the most advanced Linux platform, SUSE Linux Enterprise 12. It provides essential services, including networked storage of and access to files, print networks, driver deployment, identity-based management, and network connectivity for Windows, Mac and Linux client devices. It enables enterprises to enjoy leading-edge innovations, lower costs, and peace of mind. It features NSS - the world's most security-oriented file system, providing file access for the broadest range of clients, servers and protocols, while protecting against file corruption and simplifying file sharing among users and applications. However a number of perceptions have grown up about OES over the years. Let's dismantle some of these myths once and for all. Read on to see why Micro Focus Open Enterprise Server excels.

Myth: True or False?	Open Enterprise Server delivers:
1	*"We want native authentication and simple, client-less desktops - so must we get rid of Open Enterprise Server?"* There are certainly benefits to be had in moving to client-less network file and print services. Simplified deployments, management and troubleshooting. It works out of the box and you can leverage GPO. Have you heard about OES's **Domain Services for Windows?** It emulates Active Directory, including GPO, and leverages all existing IDs, passwords and permissions. There is no need to migrate anything and integrates with many applications and services such as VDI. It provides true client-less capabilities on the desktop and enables out of the box desktop deployments. **Simple client-less authentication works with Open Enterprise Server.**
2	*"We're moving to Active Directory, so must we move all our storage to Windows servers and NAS devices?"* The principle benefits of Active Directory are that AD is "everywhere" and most applications and services integrate with Active Directory. Fortunately OES works with Active Directory. With OES 2018 and NSS for AD there is no need to migrate any data while retaining the benefits of NSS. These include: • Rich rights model • Salvage • Fast and easy administration • Mature ACLs With OES it doesn't need to be an OR decision, it could be AND **Active Directory integration works with Open Enterprise Server**

Myth: True or False?	Open Enterprise Server delivers:

3 *"We want to virtualise our services, so does moving to Windows servers makes sense because we will get access to Hyper-V?"*

OES fully supports virtualization.

Windows Server licensing can become complex: tied to the hardware Windows Server is running on, the number of Cores and CPUs.

Open Enterprise Server includes SLES and its XEN and KVM Hypervisors. With it run an unlimited number of OES guests. Subscriptions for other operating systems are available

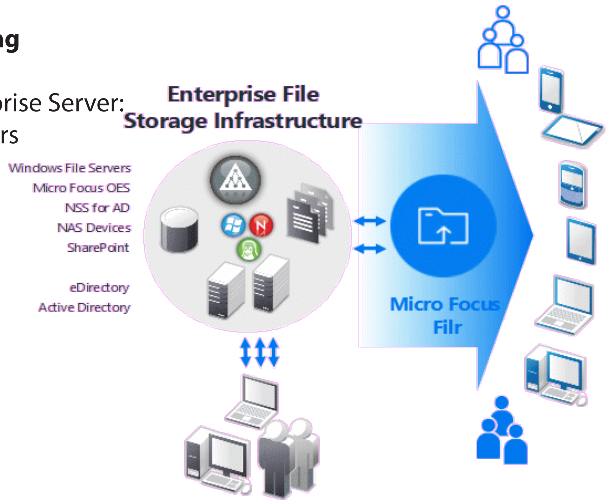
Virtualization of multiple workloads works with Open Enterprise Server

4 *"We want to securely share files internally and externally across multiple platforms and also have mobile device access. Do we need OneDrive or Box?"*

OES includes simple and secure File Sharing

Micro Focus Filr is included with Open Enterprise Server:

- Share files with internal and external users
- Leverage all existing access controls
- Stay in control of where your files are and who has access to them
- Access files from any device
- No additional costs for cloud based "maintenance" (file restores)



Securely sharing files, both internally and externals, as well as providing access from mobile devices is integrated with Open Enterprise Server

5 *"The amount of data we have is growing exponentially. Can Open Enterprise Server scale to meet our needs?"*

Current Versions of OES support a virtually unlimited amount of storage

In OES 2015 and above, the pool and volume size limit is 8 Exabytes.
You can have as many pools and volumes as you like.

OES Supports DFS, Distributed File Services. With DFS you can "join" multiple volumes together to appear as a single volume

OES can automatically tier your storage using Dynamic Storage Technology (DST). With DST you can set policies to move less-used files to a secondary volume.

Myth: True or False?	Open Enterprise Server delivers:

The Secondary storage location can have its own back-up policy, not only solving your storage problem but your backup problem as well.

With OES2018 - tiering to the cloud becomes a reality.
The user sees a merged view of both volumes together.

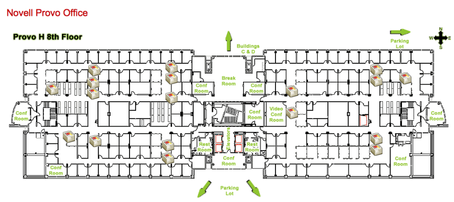
With DST you can set policies to move less-used files to a Secondary volume. The secondary storage location can have its own back-up policy not only solving your storage problem but your backup problem as well. Typically about 90% of the (stale) data can be moved to the Secondary volume.

Keeping up with today's demands for ever increasing amounts of data storage is easy with Open Enterprise Server

6 *"IP-based printing is easy, convenient, and good enough to meet my organisation's printing needs"?*

OES includes iPrint

- One of the top reasons for calls to the helpdesk are printing related
- iPrint Printer Maps are easy and intuitive and allow users to install printers and drivers with just a click
- Users always have the latest drivers
- iPrint enables accounting
- WalkUp printers let users hold and redirect print jobs to another printer
- An optional feature is that iPrint enables mobile device printing



Easy to use, self-service based printing works with Open Enterprise Server

7 *"We do daily backups. We don't need high-availability or disaster recovery?"*

Backups alone are not enough

Gartner estimates the cost of downtime for the average organisation is $5,600 per minute.
Server virtualization technologies do not entirely solve the problem. The "Service" is still unavailable if the server is corrupt, or while the repair or update work is being performed.
Open Enterprise Server (promotion) includes licenses for as many 6-node Clusters as you need to virtualise your services.

Another option is **Micro Focus Business Continuity Clustering.** This lets you create clusters of clusters, that are geographically dispersed, such that if one site is compromised, operations can continue at another location.

Highly available and replicated file and print services, works with Open Enterprise Server

8 *"We want to run on a platform that supports all of our mission-critical applications".*

Open Enterprise Server runs on SUSE Linux Enterprise Server

Myth: True or False?	Open Enterprise Server delivers:

- A leading Linux platform
- If you trust SLES for your LOB applications, why not use it for file and print as well?
- Every OES installation begins with a SLES installation
- OES is a service on SLES – just like all your other critical applications (e.g. SAP, Oracle)
- SLES is the same OS that powers many super computers and most mainframes

Run on a platform that supports mission critical line of business applications and services - choose Open Enterprise Server

9 *"As many of our desktops are Windows, we should just move to Windows servers because that's all we need to support?"*

You probably have more devices to support than you think!

- *Executives or Marketing often specify "a Mac" (41% already do).*
- *Users want to use mobile devices to do their work*
- *Some event may occasionally force people to work from home*
- *While on the road, on vacation, etc, some emergency requires you to get to your data – and all you have is a browser*

Support multiple client devices, including mobile devices, with Open Enterprise Server

10 *"OES Licensing is expensive and complex?"*

Microsoft Windows Server licensing is dependent on:
number of CPUs (2 Min) + number of Cores (16 min) + number of users + number of virtual instances
= Microsoft costs add up quickly

OES Licensing couldn't be easier:
- Only active users who access the server(s) require a license
- Servers are free
- 250,000 LDAP users are free
- Limited use license for additional LDAP users
- Inactive users (120 days) are free
- Unlimited number of promotional 6-node cluster licenses are included

Providing simple and intuitive licensing is easy with Open Enterprise Server

To summarise: OES delivers with

1. Client-less environments
2. Active Directory support
3. Virtualization capabilities
4. File sharing and mobile access
5. Host virtually unlimited amounts of storage
6. Easy to use, self-service based printing
7. High-availability and disaster recovery options
8. A world-class Linux operating system as its foundation and is supported by almost all vendors
9. Support for virtually any kind of client, even mobile
10. Easy and economical licensing

Learn more at:
www.microfocus.com/oes

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).

Filr: Adding Functionality And The Next Releases

by Devadas Kovilakath

Micro Focus Filr is a file sharing application designed from the ground up with enterprise security and management in mind, using existing filestores whether they are MS-Windows or OES based. Over the last year the team has continued to deliver many useful new capabilities and innovations via the Online Update Channel. This article reviews some of these. Please bear in mind that Filr is available in two editions, Standard and Advanced. All OES and Open WorkGroup licensees are entitled to the Standard edition, but not all features are available. (Features that are only available in the Advanced edition are indicated with a *).

All of these features, and much more, have been delivered over the Online Update Channel. However the telemetry we receive is showing that over 40 percent of customers who are entitled to use these features are not doing so because they have not configured Filr to get the updates. If you are one of these customers then have a look at the accompanying article in this magazine to see how best to set this up.

Outlook* and GroupWise integration

With files getting richer and bigger, sharing files with email clients puts a huge load on email servers, especially when they do not support a single message store. The Filr team has come up with a GroupWise integration and a plugin for Outlook which can be used – based on policies set by the Filr administrator (see figures 1 & 2) - to automatically strip message attachments, upload them to the Filr server, and add a link to the attachment file in the email's body.

This lets the email servers do what they are designed for – processing emails - and let Filr do all the heavy lifting of file access and sharing!

Figure 1: Filr Outlook policy

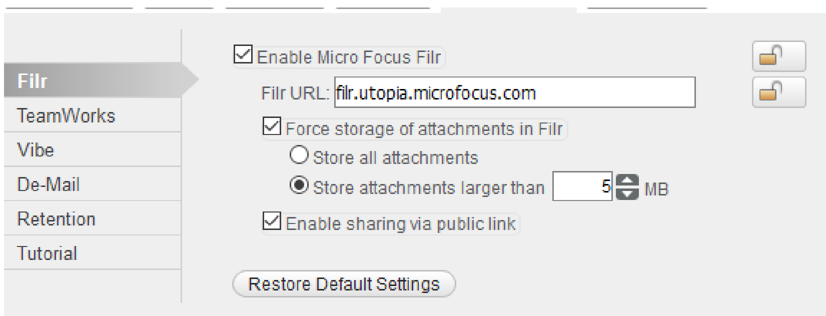


Figure 2: Filr GroupWise policy

Microsoft Office integration

If your users work mostly with Microsoft Office files – here is some great news for you. Using the MS Office plugin – your users will be able to open, save, save as and share MS Office files from the MS Office applications using Filr in the background. Filr's "Files on Demand" desktop client continues to provide you access to needed files even when offline. Welcome to the age/era of spoiling users with high productivity tools. (figure 3).

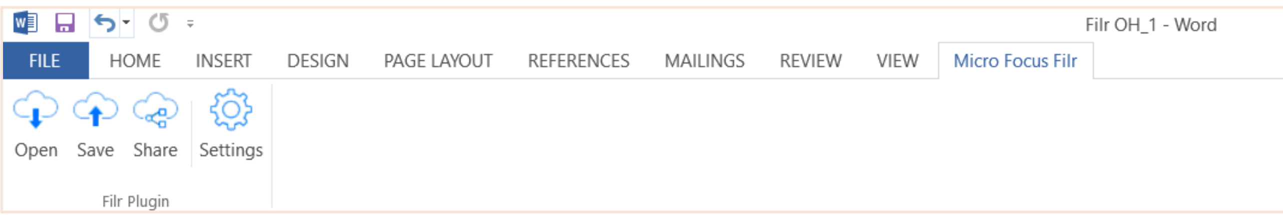


Figure 3: Filr MS office plugin toolbar

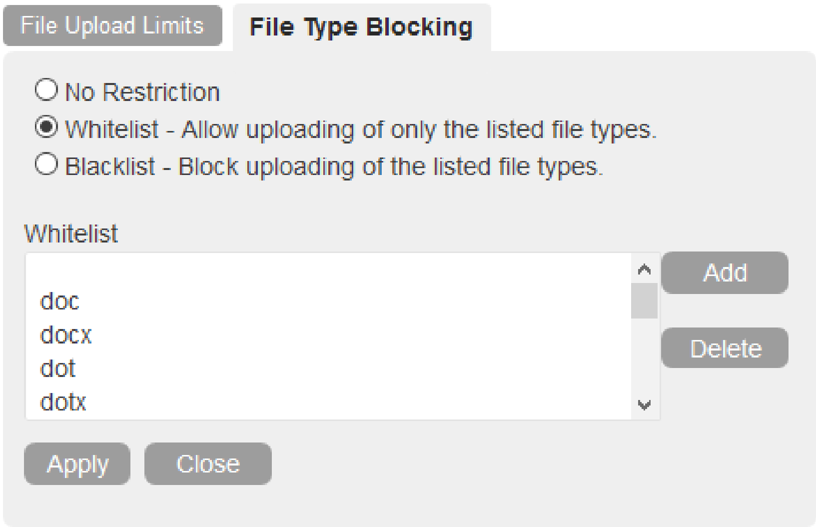


Figure 4: File Type Blocking

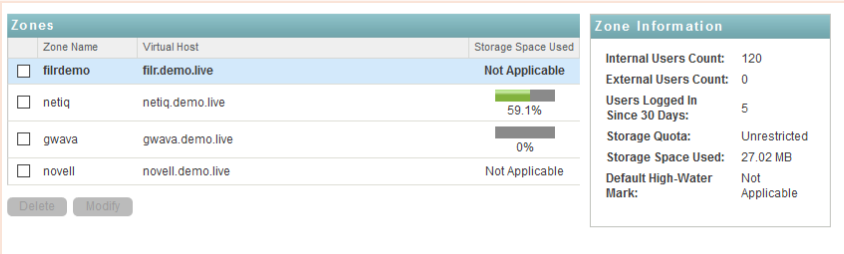


Figure 5: Zone configuration settings

Ransomware protection with File type blocking*

The Files on Demand Client we introduced in Filr 2.0 ensured that Filr users don't end up downloading all files accessible to them to their local hard disk. Automatic clean-up policies for cached files ensure that the local copies of files downloaded by users are removed after use and reduce the chance of an attack. Process blocking further mitigates the risk of ransomware attacks by ensuring that ransomware can't download online files. With Filr 3.2 checking for changes to the types of file being saved back to Filr helps further to bring down the risks associated with ransomware! (Fig 4).

Multi Factor Authentication*

The days of single factor authentication are coming to an end. With Filr 3.2 you can move beyond username and password to a more secure way to protect your sensitive information. Filr integrates with Micro Focus Advanced Authentication *(https://www.netiq.com/products/advanced-authentication)* – which specialises in multiple authentication factors so that you can now secure access to Filr further. With the Centralised policy engine, Geo-Fencing, Web-based administration and configuration portal, etc. – you get more fine-grained control of who, how, and when the authentication factors authentication should be used.

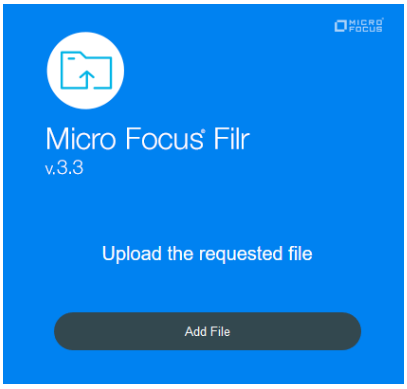


Figure 6: File Request for ad-hoc uploads

Multi tenancy with Zoning*

Partners can now host Filr for different customers in a very easy and cost effective manner. This will also help customers who have departments who wish to have a dedicated Filr system for their own use. With Filr zones that we introduced with Filr 3.3 each department and tenant will be able to manage, provision & customise their Filr system in the way they want. In addition, capabilities such as setting a storage quota so that Filr will send email notifications when the quota is close to being reached and metering will make it very easy to manage. (Figure 5).

File Request link*

This was also inspired by your many votes on the ideas portal. Often all you want is to find an easy way to get a one-off file from an external contact and you don't want them to self-register themselves on your Filr system. Filr 3.3 brought in an option for your Filr users to request non-Filr users to just upload a file anonymously (fig 6).

Linux client (Tech Preview)

When the request for a Linux Client for Filr shot up as one of the most requested ideas on the Ideas Portal – we decided to build one. We have started with a trimmed down variant of what we have for Windows and Mac Desktop. We will enhance it in the future based on your inputs. The initial release was for the SUSE Desktop and as you will see later we are adding additional distributions.

Auditing and Reporting

Administrators can now receive reports on all the files and folders shared by users who are either disabled or deleted from Filr. This will help take back or reassign control of such shares based on organisational policies.

What's coming next in Filr

This year will be an exciting time

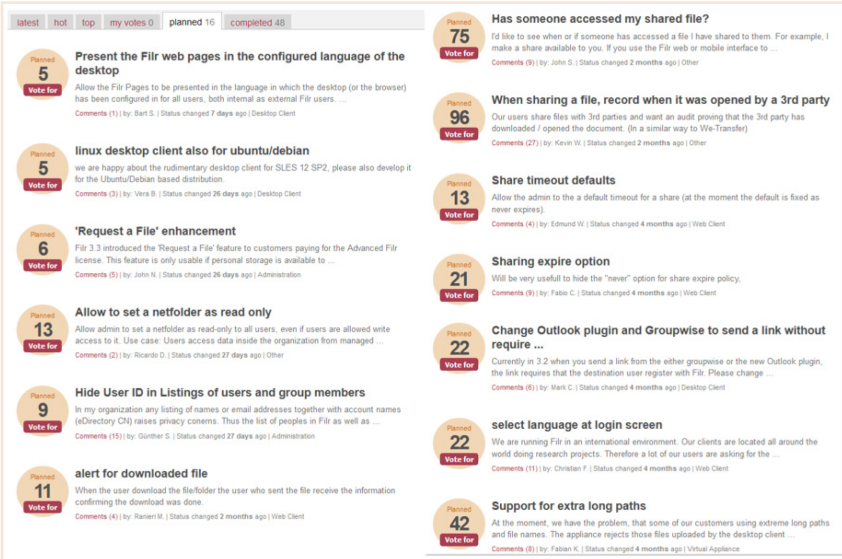


Figure 7: Planned Ideas from the portal

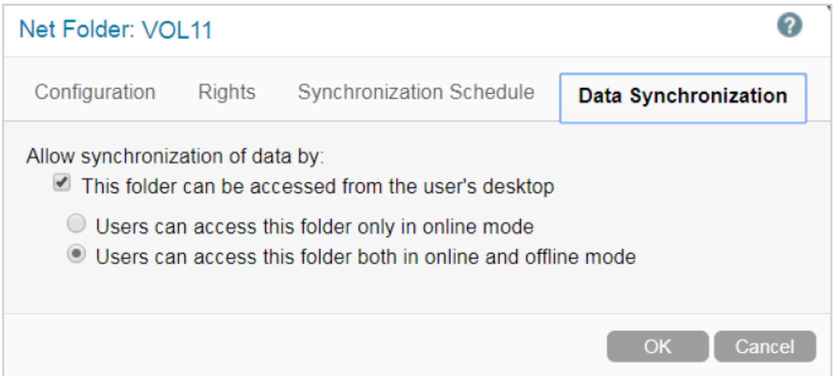


Figure 8: Data synchronisation options

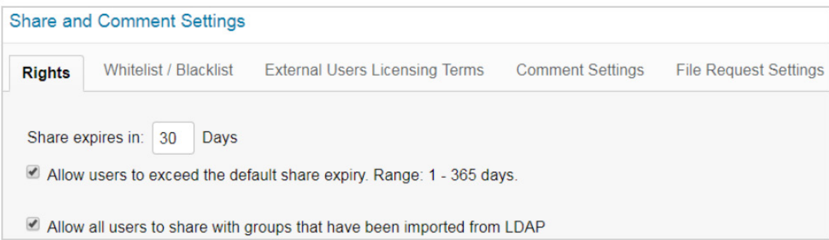


Figure 9: New share expiry settings

for Filr. The release of version 3.4 is planned for third quarter 2018 and towards the end of the year we should get Filr 4. Both these releases have some exciting features planned which we will briefly cover here.

Filr 3.4 will be soon be available. It is already in beta with many customers and partners who are signed up to the beta program. This allows them to try out the product before it is released and give feed back to the developers about the changes.

Version 3.4 is again focused on implementing enhancements from the ideas portal - https://ideas.microfocus.com/MFI/novell-filr/

Net Folder Visibility for Desktop Users*

In previous versions of Filr you could always block a Net Folder from being visible on the desktop by unchecking the option in the Data Synchronization tab on the Net Folder Configuration. In Filr 3.4 this functionality is extended to let you have an extra option to set the folder so it can only be accessed in online mode (see Figure 8) where users cannot 'make available offline' files from the folder.

Default Expiry of Shares

There is an extra option on the Rights tab under 'Share and Comment settings' (See Figure 9) that allows you to specify the default share expiry. For all new shares this will be the default. If the checkbox for 'Allow users to exceed the default share expiry' is not selected then this value can be lowered but it cannot be raised above this value.

If that check box is enabled then the value can be set over this value, but only up to a maximum of 365 days. Currently any existing shares that have an expiry date set to 'Never' will have that remain in place until the share is modified.

Conceal LDAP ID

Displaying the LDAP ID can be construed as a security risk because if an ID is known then the ID can be used by unscrupulous users to access someone else's data. A configurable option (hide.LDAPId) has been added to the ssfext.properties file (which is found in the /opt/novell/filr/apache-tomcat/webapps/ssf/WEB-INF/classes/config) to hide the LDAP IDs. Currently this file needs to be manually updated.

Web Client defaults to web browser's locale

In the past the Filr web interface would be displayed in the default language unless a user had modified their language by editing their profile. This causes issues with users, internal and external, whose native language is not the default.

With Filr 3.4 the web interface will now be displayed in the language set for the web browser. If the browser language is not one of those that is supported, then it will act as before and default to the language set on the Filr server.

Of course, should the user wish they can still override the bowser language setting and change it in their profile settings.

Linux client support for Ubuntu

In Filr 3.3 support was added for SuSE Linux. In this release there is a Technical Preview for an additional Linux platform, Ubuntu 16.04.4 LTS (Xenial Xerus). As a technical preview it is not supported.

Upgrading

The upgrade to 3.4 will be painless as it will be delivered over the online update channel. As we mentioned before the anonymous telemetry that is received shows that not everyone is keeping their 3.x systems up to date and I would urge you to set this up.

Looking ahead to version 4

The development team has starting planning for next major release of Filr: version 4.0. This will be quite a radical update with some great improvements to the product including a fresh new GUI! We will cover more on what will be in this release later in the year.

The upgrade to 4.0 will be more like upgrading in the old days because the version of SLES that the appliance runs on will be moving from 11 to 12. However, it should not be too difficult. Just take a copy of the data disk and add it to the new appliance, add a new logging disk and start it up and enter the VAAdmin password.

Devadas Kovilakath (Dev) is the Filr Product Manager. Previously he worked on iPrint, and the Novell Client in different capacities for eight years.

Updating Your Filr Installations

by Robin Redgrave

From the information that is sent back via telemetry we see that of all the Filr 3.x implementations over 40% are still running 3.0, as they have not been configured to access the online update. This means that these customers are missing out on many of the new Filr features that have been added since that release.

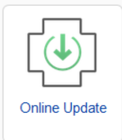
There is not actually a Filr 3.3 appliance for download. To update from Filr 3.0 you need to use the online update to bring it up to the current level. Filr 3.3.4 is the latest version and 3.4 will be released in a few weeks.

This article outlines the procedure for keeping your Filr implementation up to date by registering it on the customer portal.

Let me just take you through how to set up this important feature. First you will need to get the code from the customer portal.

Login to the Customer Center (https://www.microfocus.com/customercenter) click on software, then on the Filr 3 line and click on keys. You should see something similar as in figure 1.

Make a note of the key, which should be a fourteen character hexadecimal string. If you do not see the Key and believe you are currently under maintenance for Filr then drop an email to entitlements@microfocus.com who should be able to help.



Now login to the *Appliance Administration*, which is the https://server:9443 address. When authenticated click on the online update icon.

There is an option to use a local SMT server if you have one, but in the

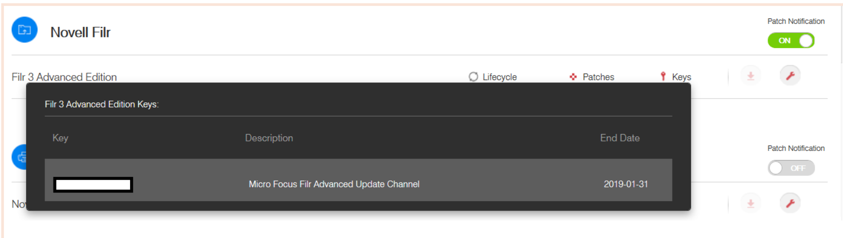


Figure 1: Getting the online update key

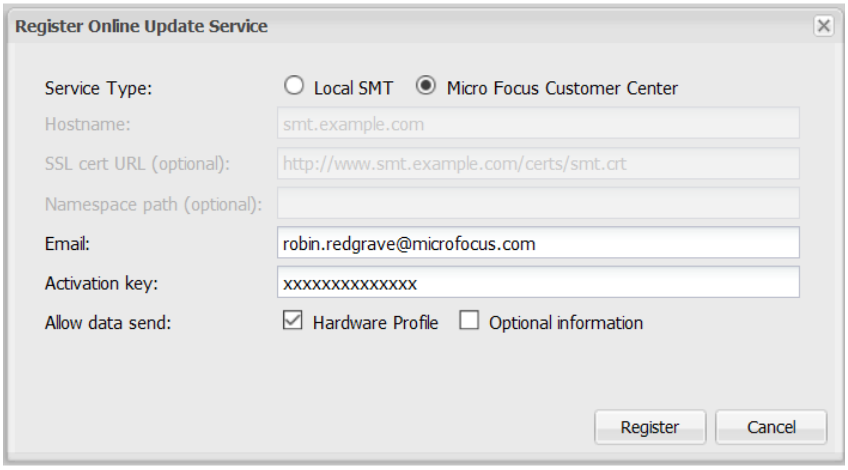


Figure 2: Configuring options for the online update.

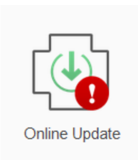
vast majority of cases you will want the updates to come from the Micro Focus Customer Center. So just select the option for that (See Figure 2).

Enter your email address and the Activation key retrieved earlier. Then just click on the option to register and sit back whilst it registers. You should then see all the patches that are available to be applied (see Figure 3).

Click on *Update Now* then check the two check boxes and click OK.

Depending on the patches being applied you may need to navigate some other dialogs before the patches are applied. Don't forget to apply patches to all the appliances in your environment, not just the web appliance. The search and index appliances will need patching as well, but be aware that if there is a patch for one appliance type there may not be one required for the other appliance types.

At any time in the future when there is a new update to apply you will see a notification when you login to the appliance administration.

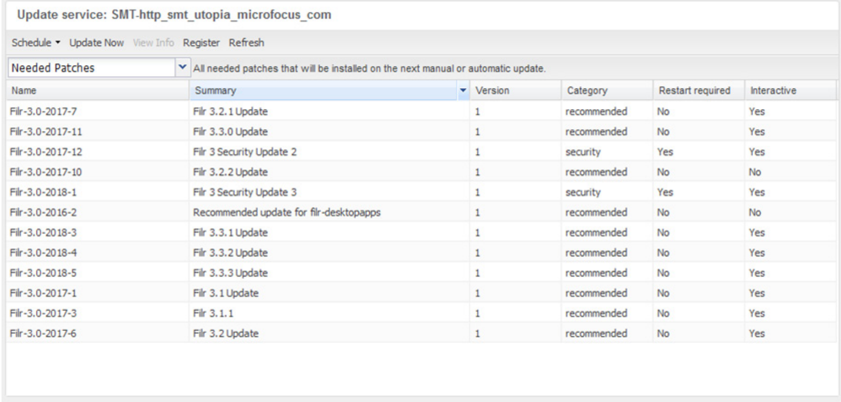


Alternatively you can set an automatic schedule for them to be applied.

For further information have a look at this cool solutions article:

https://www.novell.com/communities/coolsolutions/registering-and-updating-using-filrs-online-update-channel/

My understanding is that the 149 patch it talks about is now integrated into the updates that are pulled down. If you use SUSE Manager then there are instructions available at:



Update service: SMT-http_smt_utopia_microfocus_com

Schedule ▾ Update Now View Info Register Refresh

Needed Patches — All needed patches that will be installed on the next manual or automatic update.

Name	Summary	Version	Category	Restart required	Interactive
Filr-3.0-2017-7	Filr 3.2.1 Update	1	recommended	No	Yes
Filr-3.0-2017-11	Filr 3.3.0 Update	1	recommended	No	Yes
Filr-3.0-2017-12	Filr 3 Security Update 2	1	security	Yes	Yes
Filr-3.0-2017-10	Filr 3.2.2 Update	1	recommended	No	No
Filr-3.0-2018-1	Filr 3 Security Update 3	1	security	Yes	Yes
Filr-3.0-2016-2	Recommended update for filr-desktopapps	1	recommended	No	No
Filr-3.0-2018-3	Filr 3.3.1 Update	1	recommended	No	Yes
Filr-3.0-2018-4	Filr 3.3.2 Update	1	recommended	No	Yes
Filr-3.0-2018-5	Filr 3.3.3 Update	1	recommended	No	Yes
Filr-3.0-2017-1	Filr 3.1 Update	1	recommended	No	Yes
Filr-3.0-2017-3	Filr 3.1.1	1	recommended	No	Yes
Filr-3.0-2017-6	Filr 3.2 Update	1	recommended	No	Yes

Figure 3: Available patches

Figure 4: Updating

https://www.novell.com/communities/coolsolutions/integrate-filr-3-suse-manager-3/

Major version upgrades

I suspect that when Filr 4 is released towards the end of the year, that it will require an upgrade of the whole appliance as the underlying operating system is changing from SLES 11 to SLES 12.

However, I suspect that the upgrade will be similar to the previous procedure for moving from one major version to another. You will just need to take a copy of the data disk and add it to the new appliance, add a new logging disk, start it up and enter the VAAdmin password.

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.

Embrace the Digital Workspace

Micro Focus

Enabling the workspace through Unified Endpoint Management

Automation | Configuration
Configuration Management, Endpoint Security, Mobile Workspace, Service Desk, Patch Management, Desktop Containers, Asset Management

+

Single Pane Of Glass
The ZENworks Control Center / Common End User Portal

+

Security
Full Disk Encryption, Endpoint Security, Mobile Workspace, Desktop Containers

+

Compliance
Asset Management, Patch Management, FDE, Endpoint Security

+

User Self-services
Service Desk, Mobile Workspace, Desktop Containers

microfocus.com/products/zenworks

MICRO FOCUS®