**INF113 System Monitoring Pilot**

**Recommendations Report**

**Contributors**

|  |  |  |
| --- | --- | --- |
| **Name** | **Role** | **Sign Off** |
| Colin Watt | IS Apps – Project Manager | 22/08/16 |
| Maurice Franceschi | IS Apps – Programme Manager | 22/08/16 |
| Stefan Kaempf | IS Apps – Project Sponsor / Programme Owner | 12/08/16 |
| Fiona Lawson | IS ITI – Enterprise Services | 22/08/16 |
| Murray Dippie | IS ITI – Enterprise Services |  |
| Garry Scobie | IS ITI – Enterprise Services |  |
| Graeme Wood | IS ITI – Enterprise Services | 22/08/16 |
| Martin Campbell | IS ITI – Enterprise Services | 12/08/16 |
| Iain Fiddes | IS Apps – Head of Development Services |  |
| Heather Larnach | IS Apps – Technical Management Team Manager |  |

|  |  |
| --- | --- |
| **Version** | 1.2 for review |
| **Date** | 22 August 2016 |
|  |  |

# Executive Summary

Having encountered a number of technical and non-technical challenges establishing a limited pilot of SCOM on the UniDesk and Learn infrastructure, the project team agree that despite the hopes of the evaluation done on INF107 in 2014/15 the SCOM product has not lived up to its promise to provide the “Single Pane of Glass” view for technical staff, and the out of the box functionality across the board falls short of what is required in order to recommend rolling out across IS services for technical staff and service owners in various IS divisions.

The project team agree that the pilot has failed to deliver because either the scope (monitoring across the breadth and depth of the IS infrastructure, and providing dashboard capability on top) was too ambitious and / or the product does not provide what we need at the technical level.

The following recommendations are made, based on piloting SCOM against the selected Windows and Linux based services:

* Consider changing the scope of what is delivered. For example:
1. Splitting scope into separate projects to address the monitoring and unified presentation layers.
2. Defining a detailed set of requirements for a monitoring tool that can be used to progress a procurement.
3. Managing a project to develop feeds from existing monitoring tools into a normalised form for presentation by a dedicated presentation / dashboard tool for service owners.
* SCOM continue to be used in specific teams, for specific services, and specific technologies (most likely where Windows based services are monitored).
* IS effort not be used to roll out SCOM across IS either generally or for high priority services (this means that the INF project planned for 2016/17 to roll out SCOM based on a successful pilot will now not be initiated).
* This recommendation report is communicated to IS directors (Applications and IT Infrastructure) and a meeting is arranged by to review and discuss the report and future plans regarding monitoring within IS. This meeting should establish the plans for IS’s monitoring and give a steer what directions we should go. Possible directions are:
1. Do nothing. Keep a large number of reporting tools and report team by team with no cross team and section reporting in place.
2. Introduce new tools and replace old tools but not across IS, but across specific functions or layers. This may address some of the difficulties that there are very few tools able to cover all aspects from network to user service dashboards. It is likely that this will separate into the following components: Networks, Infrastructure, Application, Service.
3. Implement a cross IS tool which will cover all aspects of monitoring. This will require a full procurement and large engagement from IS over the next years.
* That the following recommendation from INF107 *not* be actioned : *“If the SCOM product pilot is unsuccessful, the project team would require to re-evaluate the other incumbent solutions and/or third party products in order to make a required recommendation.”*

**Background**

IS manages a large number of high priority services for the University with 24x365 uptime and 99.9% availability expectations. Over recent years the number of infrastructure components involved in providing these priority services has grown significantly and to a level where manual checks are no longer feasible. Additionally, the numbers of lower priority but high value services has grown at an even greater rate over the same period.

In 2014/15 the INF107 project was undertaken to perform an appraisal on automated monitoring solutions and deliver recommendations on how monitoring across IS should be taken forward.

The INF107 project made the following recommendations:

* SCOM is trialled as a Pilot and a formal process of technical evaluation and acceptance is carried out to ensure that the product is suitable and delivers the desired benefits and outputs.
* The Pilot should also trial Organisational Changes for a chosen number of services. Changes should be based on ITIL best practice and drawn up by the project team potentially using external ITIL expertise.
* Should the Pilot prove to be successful the University goes on to fully adopt the ITIL changes recommended and validated by the pilot and fully deploys the chosen monitoring solution.
* If the SCOM product pilot is unsuccessful, the project team would require to re-evaluate the other incumbent solutions and/or third party products in order to make a required recommendation.
* As part of the Pilot the panel recommends that an ITIL maturity assessment be carried-out at the University and that recommendations from that review be assessed.
* The necessary staff and technical resources should be provided to ensure that both organisational change and the technical platform deliver a solution that optimises our delivery of services to the business.

The INF113 project was therefore established in 2016/17 to pilot Microsoft’s SCOM ([System Center Operations Manager](https://en.wikipedia.org/wiki/System_Center_Operations_Manager)) which is part of its [System Center](http://www.microsoft.com/en-us/server-cloud/products/system-center-2012-r2/); it was agreed at the planning stage with the Project Sponsor and the Director of IS Infrastructure that the project would focus on piloting the product, and that the recommendations relating to organisational changes and roles to support the pilot (and ITIL maturity assessment), would be descoped from the project, as these would be covered by separate initiatives within IS as part of the CIO’s focus on service management.

It was agreed that SCOM be piloted with three types of service:

* A Windows based service (UniDesk)
* A Linux based service (Learn)
* A non-IS service (eFinancials)

The intention was to determine the product’s capability to provide a “single pane of glass” view for technical staff, and to provide dashboard capability for end users such as Service Owners across IS.

## Detail to support the recommendations

SCOM was initially configured on the UniDesk service as it was considered that a Windows based service would be more straightforward to set up than a Linux based one and would offer a good learning opportunity on the tool.

“Out of the box”dashboard capability was delivered as part of this project milestone so that this could be evaluated. The monitoring and dashboards were positively received but a number of issues were uncovered during this and the work done on the pilot for the second (Linux based) service.

A Microsoft consultant visited and worked through a number of issues with the delivery team and provided support and guidance on SCOM configuration.

The key issues from the first pilots, and the Microsoft consultation were:

* SCOM provides good monitoring for Windows servers and Microsoft applications. Monitoring outside of this requires third party management packs (MPs) eg. Veeam for VMware, or custom written management pack for specialist applications eg. Topdesk, timetabling. Buying third party MPs increases the total cost of ownership of SCOM, and writing our own MPs is a complex and time consuming task. Currently we lack in-house skills in this area.
* Microsoft’s recommended approach is to set up distributed applications which is more complex and time consuming that originally envisaged. The engineer said that it typically takes approx three weeks to fully set-up monitoring for a service. That is three weeks per service, which is a significant investment in time and resource; for example on this basis full set up of SCOM for the top ten priority services would take the best part of one year assuming 1 x fte full time available in ITI, and this is in-house experience that is currently not present.
* Producing dashboards and distributed applications are quite difficult to produce ‘out the box’ so 3rd party companies have produced products to fill the gap. This potentially introduces additional complexity and increases total cost of ownership.
* The dashboards within SCOM are limited. ‘Drill down’ is not available out of the box; The recommendation from Microsoft is to use Visio along with the SCOM data connector for Visio to pull live data from SCOM and populate health states into Visio diagrams and provide ‘drill downs’.
* The built-in SCOM diagram views are static and not very flexible; they cannot be added to a dashboard.
* Monitoring Linux based services was originally hoped to be a ‘light touch’ monitoring, but is now evident that it will be a duplication of effort to monitor with SCOM and ZenOSS as SCOM cannot aggregate data from ZenOSS.
* Installation of SCOM agents on Linux servers will use the MS Linux Management Pack and provide monitors for the Linux OS. Most applications running on Linux will require a third party MP (these will often have a cost).
* There are legitimate security concerns that need to be addressed. Most Unix/Linux MPs have a requirement for root access.
* Basic monitoring requires lower permissions but can be complex to set up; the VManagement pack can monitor Virtual Machines using VMWare tools – although this would be unable to monitor physical servers without the installation of agents.
* SCOM can provide a level of network monitoring. However the functionality that maps servers to switch ports works using network discovery. If a vm is migrated to a new VMware host the switch port mapping does not automatically update. A new network discovery job would need to be run. The recommendation is not to run network discovery more than 1 to 2 times a week, meaning that the data could often be out of date, therefore the network monitoring is not fit for the purpose we want.
* Another type of network monitoring could be achieved using synthetic transactions to check server and port availability from different locations. Microsoft has a Global Service Monitoring service, which allows use of servers across the world as watchers for synthetic transactions; this is available free if you have software assurance, otherwise it is a paid for service.
* There is no out of the box SNMP support for monitoring Linux; Linux servers can be added as a device and then discoveries, rules and monitors would have to be built to monitor anything (creating a custom management pack for the servers, for which no in-house experience exists)
* Microsoft provide connectors for SCOM and SharePoint allowing data to be published to a SharePoint site, however this requires server-side code, therefore would not be possible on Office 365 and would instead require a separate SharePoint Enterprise instance.
* Microsoft’s Internet Explorer is the only officially supported browser for the web console. This is a significant showstopper for adoption og SCOM within the University.

**Overcoming technical and non-technical obstacles**

It became apparent to the project team that with support only for Internet Explorer, and limited out of the box dashboard capability, that deploying SCOM across IS would require workarounds for technical and non-technical obstacles which would not necessarily be easy to achieve or enforce in the University. For example, providing monitoring information which could only be consumed by service owners using Internet Explorer on a Windows desktop would not allow us to reach the target audiences across the University.

It was agreed therefore that it would be worthwhile using project budget to evaluate 3rd party tools which had emerged specifically to address SCOM’s shortcomings, rather than halting the pilot early.

The project team took advantage of a one month free evaluation of [SquaredUp.com](https://squaredup.com/)’s product. SquaredUp provides a responsive HTML5 Web console, a Dashboard designer, and Visio plugin. SquaredUp facilitated easier development of more sophisticated dashboards and provided a means to deal with the Internet Explorer restrictions, as the product provides support for multiple browsers. Feedback to the dashboards was positive and the project team agreed that using SquaredUp alongside SCOM would at least provide an easier way to develop dashboard capability and the means to distribute data to service owners.

However, it is clear that despite having the means to develop and distribute dashboards to service owners, there are a number of shortcomings in the underlying functionality of the SCOM product which mean that it falls short of what is required for technical staff and therefore the project team cannot recommend further effort is invested in deploying it for monitoring of University services. The relevant issues here are:

* The inability to consume data from existing incumbent monitoring tools which requires “double-monitoring” (increased traffic and load) and introduces the possibility that separate tools may report inconsistent data and trigger conflicting statuses (eg SCOM reports service is GREEN, however another more specialised tool reports an aspect of the service as RED) resulting in confusion, and staff resource being consumed manually checking. This undermines the confidence that our technical staff have in the tools they use, and in their ability to reliably and professionally manage infrastructure and key services.
* With SCOM’s inability to aggregate data from incumbent monitoring tools, its shortcomings on monitoring of MySQL, Oracle, JVMs, JMX, LDAP, DNS, SMTP, SNMP mean that the product is not capable of providing information consistent with incumbent monitoring tools and therefore would be unable to replace them.
* The requirement to install agents for full capability on Linux infrastructure presents a security risk which IS ITI Enterprise Services consider unacceptable.
* The prospect of investing significant staff effort across IS to implement a solution which does not provide the answer to the monitoring problem.

**Conclusions and Recommended next steps**

In conclusion, the reviews of the pilot have stimulated a great deal of discussion on the technical and non-technical challenges presented by the scope of this initiative. The project team feel that there is a much better understanding of the capabilities of the tool, and of what is required by various audiences within the University. The project team feel that at this time SCOM cannot be considered as fit for purpose across the breadth and depth of our infrastructure and therefore recommends that no further effort be invested in pushing SCOM for deployment for IS service owners due to the technical shortcomings, complexity, and the total cost of ownership.

As well as the requirement for accurate and reliable infrastructure and application level monitoring, the desire for service level dashboard capability remains and is real.

The project team have discussed how the scope could be broken down in order that, if appropriate, separate projects could be used to deliver capability against the different requirements needed to address the needs of technical, service oriented, and non-technical staff.

The following recommendations are made, based on piloting SCOM against the selected Windows and Linux based services:

* Consider changing the scope of what is delivered. For example:
1. Splitting scope into separate projects to address the monitoring and unified presentation layers.
2. Defining a detailed set of requirements for a monitoring tool that can be used to progress a procurement.
3. Managing a project to develop feeds from existing monitoring tools into a normalised form for presentation by a dedicated presentation / dashboard tool for service owners.
* SCOM continue to be used in specific teams, for specific services, and specific technologies (most likely where Windows based services are monitored).
* IS effort not be used to roll out SCOM across IS either generally or for high priority services (this means that the INF project planned for 2016/17 to roll out SCOM based on a successful pilot will now not be initiated).
* This recommendation report is communicated to IS directors (Applications and IT Infrastructure) and a meeting is arranged by to review and discuss the report and future plans regarding monitoring within IS. This meeting should establish the plans for IS’s monitoring and give a steer what directions we should go. Possible directions are:
1. Do nothing. Keep a large number of reporting tools and report team by team with no cross team and section reporting in place.
2. Introduce new tools and replace old tools but not across IS, but across specific functions or layers. This may address some of the difficulties that there are very few tools able to cover all aspects from network to user service dashboards. It is likely that this will separate into the following components: Networks, Infrastructure, Application, Service.
3. Implement a cross IS tool which will cover all aspects of monitoring. This will require a full procurement and large engagement from IS over the next years.
* That the following recommendation from INF107 *not* be actioned : *“If the SCOM product pilot is unsuccessful, the project team would require to re-evaluate the other incumbent solutions and/or third party products in order to make a required recommendation.”*