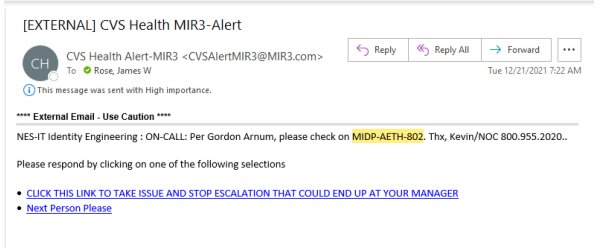
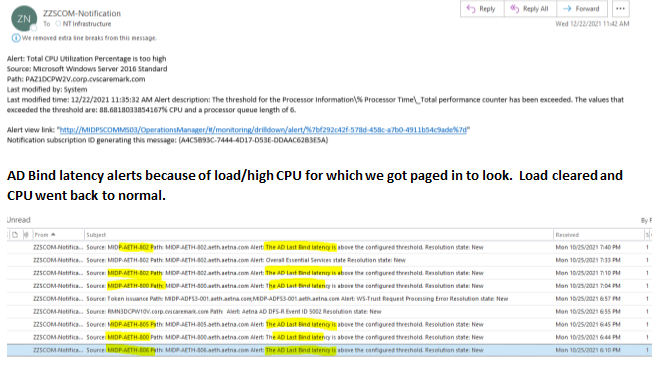
|  |
| --- |
| **Audit Name: Active Directory**  **Audit Number: 21121**  **Prepared by: Seun Mafi**  **Date Completed: 2/9/2022** |

|  |  |
| --- | --- |
| Control & Sample Information | |
| Control | E2.2 – Event Monitoring |
| Sample Number | IA sampled 4 out of the 9 actionable SCOM event alerts received by the AD infrastructure team in the last 1 month and tested to determine adequacy and effectiveness of this control |
| Supporting Documentation Received From | James W. Rose (Senior Engineer Advisor) |
| Received Date | 12/29/2021, 01/31/2022, 2/2/2022, 2/4/2022, 2/8/2022 |
| Purpose of the Test | The purpose of this test is to ensure that SCOM event was identified and communicated to the AD infrastructure team, AD infrastructure team performed root cause analysis for the sampled events, and issues and remediation was documented and made available to be viewed by all stakeholders. |
| Source Files | [UID #13200](https://cvshealth.auditboardapp.com/download?file_id=159360&name=UID%20%2313200.docx)  [Task15133 – E2.2 SCOM Event Logs](https://cvshealth.auditboardapp.com/download?file_id=160160&name=Task15133%20-%20E2.2%20SCOM%20Event%20Logs.docx)  [Task15416 – E2.2 SCOM Alerts Follow Up](https://cvshealth.auditboardapp.com/download?file_id=161403&name=Task15416%20-%20E2.2%20-%20SCOM%20Alerts%20Follow%20Up.docx)  [Task15416 – E2.2 Full Population SCOM Alerts](https://cvshealth.auditboardapp.com/download?file_id=161584&name=Task15416%20-%20E2.2%20-%20Full%20Population%20SCOM%20Alerts.xlsx)  [Task15443 – E2.2 SCOM Alert Remediation](https://cvshealth.auditboardapp.com/download?file_id=161624&name=Task15443%20-%20E2.2%20SCOM%20Alert%20Remediation.docx)  [Task15416 – E2.2 – SCOM Alerts (IA Analysis)](https://cvshealth.auditboardapp.com/download?file_id=162033&name=Task15416%20-%20E2.2%20-%20SCOM%20Alerts%20(IA%20Analysis).xlsx) |

**Attribute 1: The SCOM event was identified and communicated to the AD infrastructure team.**

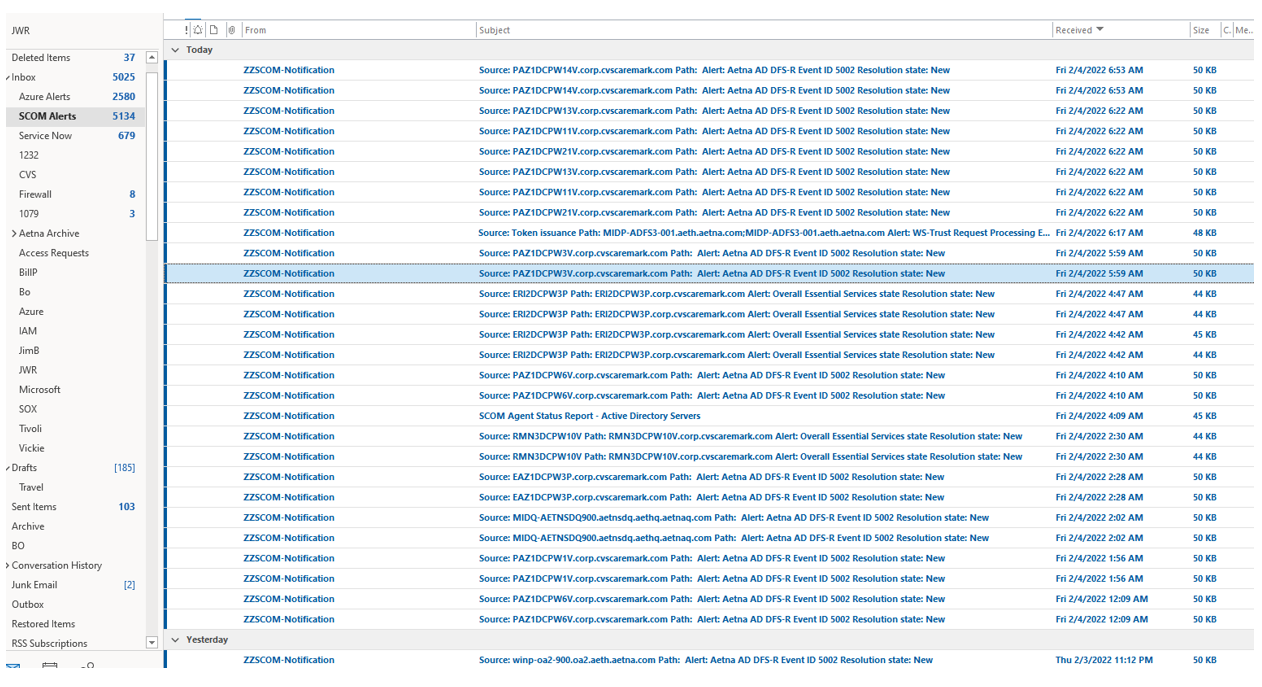
On 01/31/2022, IA received from James Rose (Senior Engineering Advisor) evidence showing SCOM alerts and Tivoli alerts received by AD infrastructure team. During a follow up meeting scheduled with James Rose to further understand the details of the evidence provided, IA gathered that the AD infrastructure team receive email notifications generated from CVS health Alert-MIR3 (Tivoli) and ZZSCOM-Notification. ([UID #13200](https://cvshealth.auditboardapp.com/download?file_id=159360&name=UID%20%2313200.docx)) *See evidence below:*





The email alerts generated from both CVS health Alert-MIR3 (Tivoli) and ZZSCOM-Notification occur as a result of a password reset process, changes on server being processed, high CPU usage or memory issues and application related issues. James also explained that most of the email alerts received (about 99%) are informational, and therefore no action was required to resolve these alerts as they were automatically cleared and system operated as normal; however, for the alerts received that required an action to be taken, a change record was created, and actions were taken to determine the root cause of the alert, and remediation performed to resolve the issue.

Jim provided a screenshot evidencing the SCOM event alerts received by the AD infrastructure team. ([Task15416 – E2.2 SCOM Alerts Follow Up](https://cvshealth.auditboardapp.com/download?file_id=161403&name=Task15416%20-%20E2.2%20-%20SCOM%20Alerts%20Follow%20Up.docx)) *See evidence below:*



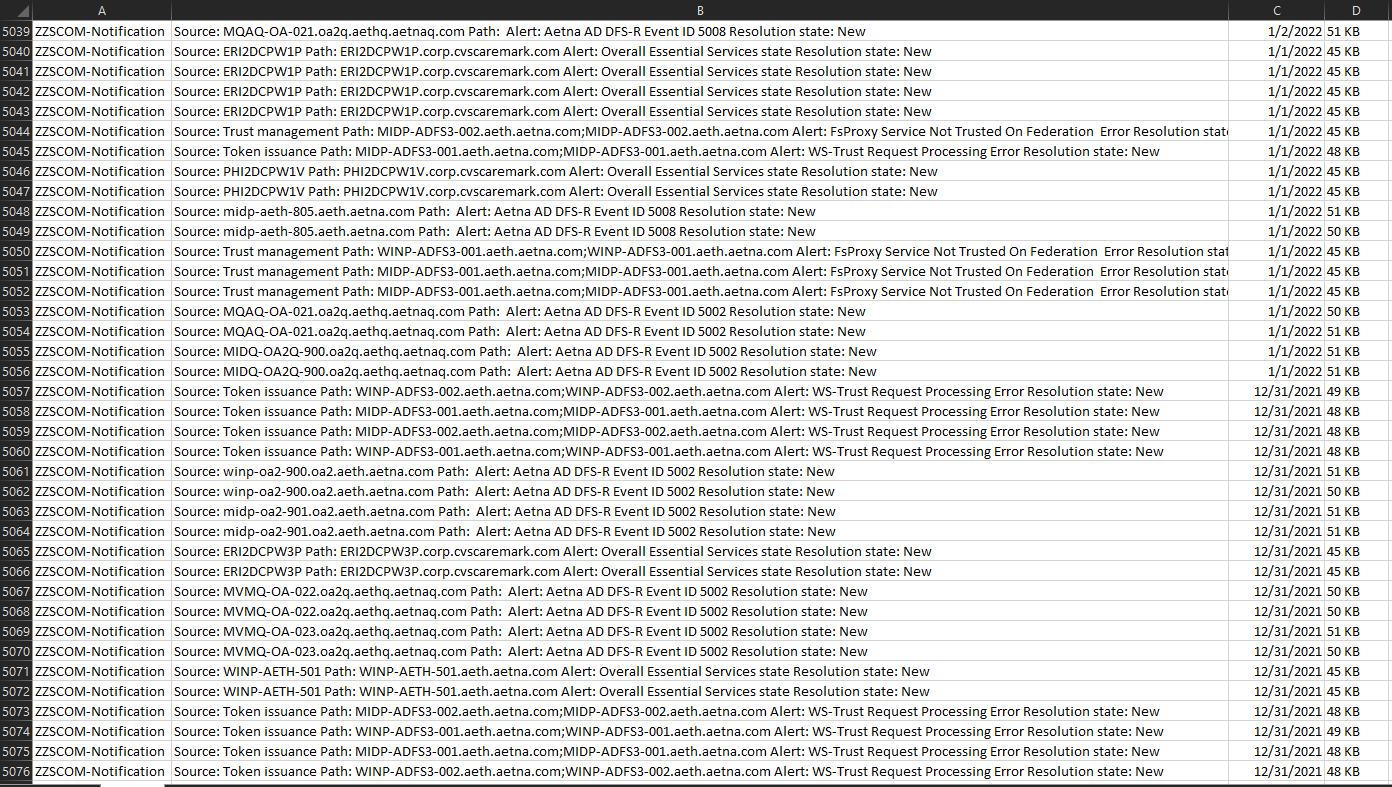
IA gained assurance that SCOM events were identified and communicated to the AD infrastructure team.

Attribute satisfied.

**Attribute 2: The AD Infrastructure team performed root cause analysis for the sampled events.**

IA gaining an understanding that majority of the alerts received by the AD Infrastructure team are non-actionable items which do not require a root cause analysis performed as they were automatically resolved and cleared. A large amount of these non-actionable SCOM event alerts include passport reset notification requiring no action to be taken. For this testing, IA requested for a full population of all actionable SCOM event alerts which have a change record for the past 1 month.

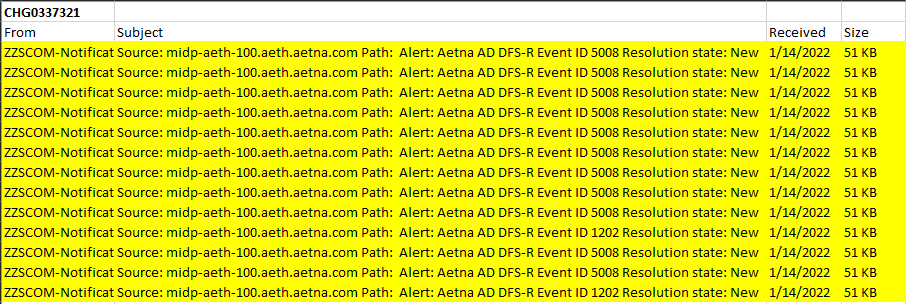
On 2/4/2022, IA received from James Rose (Senior Engineering Advisor) evidence of all the SCOM alerts received by the AD infrastructure team from 12/29/2021 through 2/4/2022 ([Task15416 – E2.2 Full Population SCOM Alerts](https://cvshealth.auditboardapp.com/download?file_id=161584&name=Task15416%20-%20E2.2%20-%20Full%20Population%20SCOM%20Alerts.xlsx)) *See evidence below:*



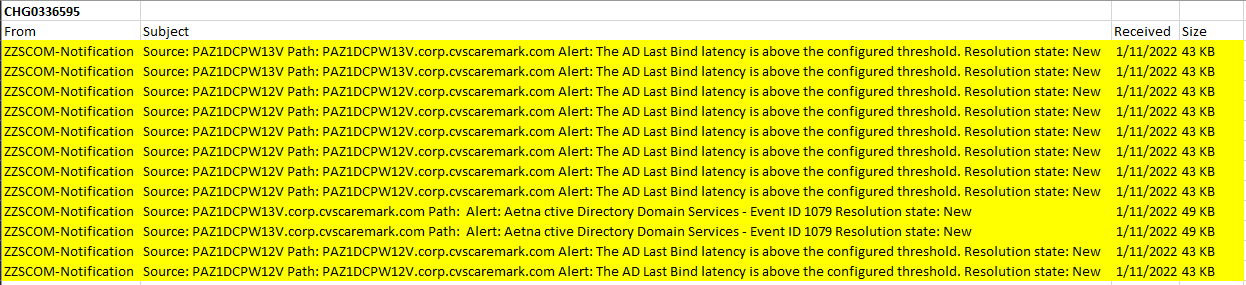
Given the high volume of SCOM alerts received by the AD infrastructure team on a daily basis, and also given these SCOM event alerts are adhoc; based on methodology requiring a sample of 25 which is 10% of 250 when population size is in excess of 250; in order to gain assurance on testing sample, IA selected a sample of 25 SCOM events alerts which are tied primarily to 2 change tickets dated on 1/11/2022 and 1/14/2022. IA also noted that the SCOM events captured in the sampled population size included a large volume of repetitive events, as most of these events were not unique occurrences.

IA conducted additional analysis on the full population provided by James ([Task15416 – E2.2 – SCOM Alerts (IA Analysis](https://cvshealth.auditboardapp.com/download?file_id=162033&name=Task15416%20-%20E2.2%20-%20SCOM%20Alerts%20(IA%20Analysis).xlsx)). The analysis includes all SCOM event alerts and associated change tickets received by the AD infrastructure team for dates 1/11/2022 and 1/14/2022. *See evidence below:*

1/14/2022 SCOM Alerts (13 events) – Associated change ticket (**CHG0337321**)

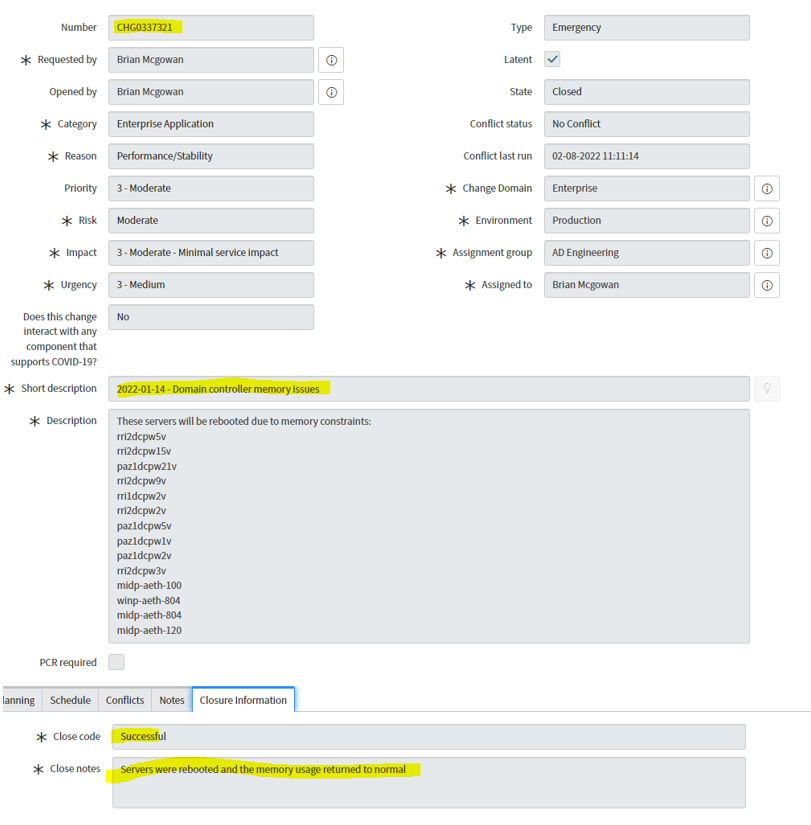


1/11/2022 SCOM Alerts (12 events) – Associated Change ticket (**CHG0336595**)

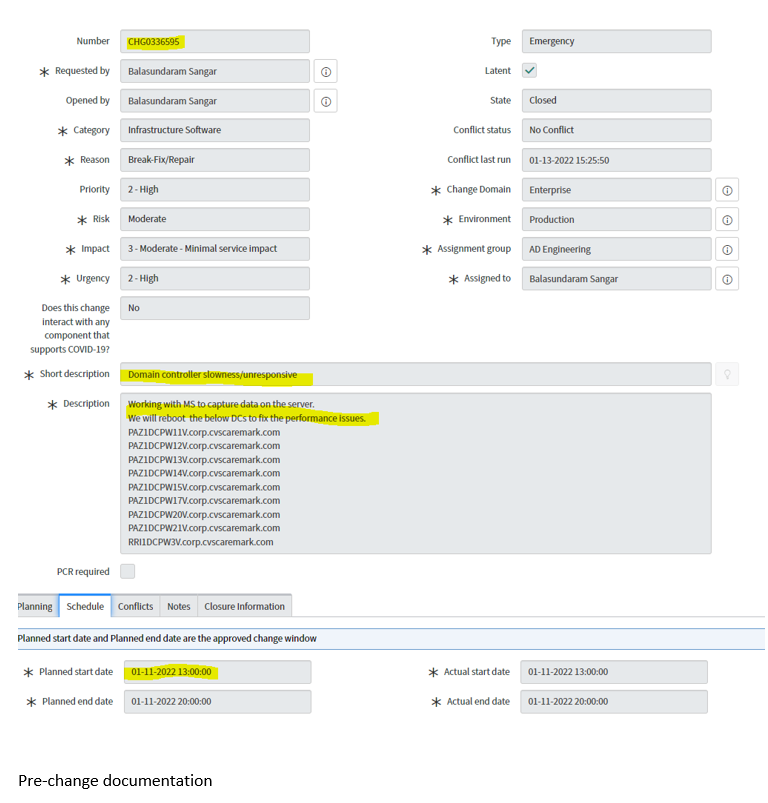


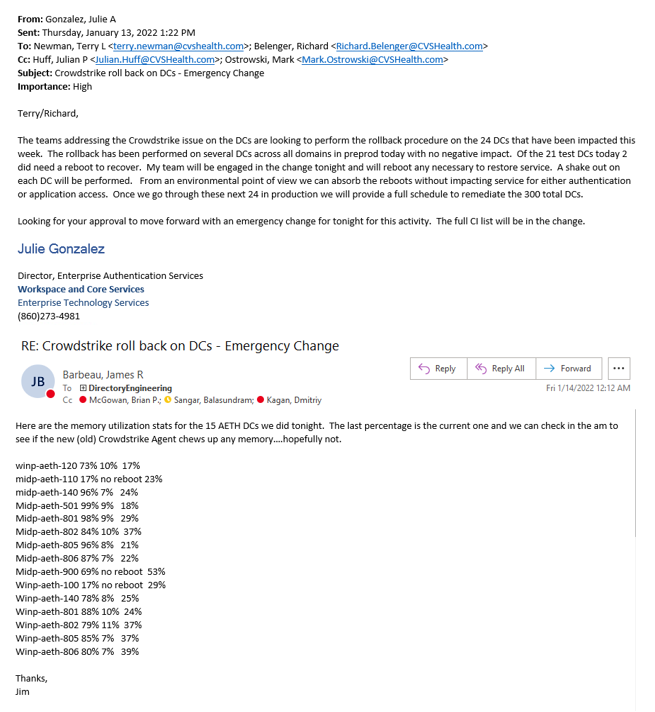
Additionally, IA reviewed the records of the associated change tickets tied to these sampled SCOM event alerts for further testingh. ([Task15443 – E2.2 SCOM Alert Remediation](https://cvshealth.auditboardapp.com/download?file_id=161624&name=Task15443%20-%20E2.2%20SCOM%20Alert%20Remediation.docx)) *See evidence below:*

1. CHG0337321 – 01/14/2022
2. CHG0336595 – 01/11/2022
3. CHG0337321



1. CHG0336595





IA observed that each of the SCOM event alerts sampled have an associated change ticket which give a description of the root cause (issue) and a remediation process that was executed by the AD infrastructure team to fix the identified issue.

IA gained assurance that the AD infrastructure team performed root cause analysis for the sample events.

Attribute satisfied.

**Attribute 3: The Issue, RCA and resolution was documented and made available for all stakeholders to see.**

As documented in the evidence provided in Attribute 2, IA observed that the change records associated with each of the sampled SCOM event alerts contained details of the identified issue, and process to be implemented in fixing the issue (resolution). Furthermore, James Rose (Senior Engineering Advisor) included screenshots evidencing email communication that occur among the AD infrastructure team when root cause analysis and remediation were performed. IA gained assurance that records of change tickets tied to SCOM event alerts, root cause analysis, and email communication generated in order to resolve SCOM event alerts are documented and can be readily accessible.

Attribute satisfied.

**Conclusion:**

After testing the evidence and artifacts provided, IA gained assurance that SCOM events were identified and communicated to the AD infrastructure team, root cause analysis was performed by the AD infrastructure team for SCOM events that required action to be taken, and identified issues and resolution were documented and made readily accessible.