# Lab Answer Key: Module 12: Monitoring and troubleshooting Microsoft Office 365

# Lab: Monitoring and troubleshooting Office 365

## Exercise 1: Monitoring Office 365

#### Task 1: Send an email to a nonexistent domain

1. On LON-CL1, on the taskbar, click **Microsoft Edge**.
2. Browse to **https://portal.office.com/**, and then sign in as **holly@gsp.Adatumvsxxxx.virsoftlabs.com** by using the password you created in Module 1.
3. Click **Mail**, and then click **New**.
4. In the **To** text box, type **user@alt.none**.
5. Enter a subject and some body text, and then click **Send**.

#### Task 2: Track mail delivery

1. Wait for the delivery failure message to appear.
2. Note the reason for the failure ("The domain name in the email address is incorrect.").
3. Select the body text of the message, including the phrase "**Generating server**" down to "**X-OriginatorOrg: gsp.Adatumvsxxxx.virsoftlabs.com** " and then press Ctrl+C to copy it to the Clipboard.
4. In Microsoft Edge, press Ctrl+T to create a new tab.
5. In the new tab, browse to **https://testconnectivity.microsoft.com**.
6. On the **Microsoft Remote Connectivity Analyzer** page, click the **Message Analyzer** tab.
7. Under Message Header Analyzer, paste the message, and then click **Analyze headers**.
8. Note the diagnostic information and the time taken for the message to be rejected.
9. Click **Clear** to reset the Message Header Analyzer.

#### Task 3: Send an email to a nonexistent user

1. In Microsoft Edge, click Holly's **Mail** tab.
2. Click **New**, and then in the **To** text box, type **difflop48999@outlook.com**.
3. Enter a subject and some body text, and then click **Send**.

#### Task 4: Track mail delivery

1. Wait for the delivery failure message to appear.
2. Note the reason for the "550 Requested action not taken: mailbox unavailable" failure.
3. Select the body text of the message including the phrase "**Generating server**" down to "**X-OriginatorOrg: gsp.Adatumvsxxxx.virsoftlabs.com** " and then press Ctrl+C to copy it to the Clipboard.
4. In Microsoft Edge, switch to the **Microsoft Remote Connectivity Analyzer** tab.
5. On the **Microsoft Remote Connectivity Analyzer** page, ensure that you are on the **Message Analyzer** tab.
6. Under Message Header Analyzer, paste the message, and then click **Analyze headers**.
7. Note the diagnostic information and the time taken for the message to be rejected.
8. Close the **Microsoft Remote Connectivity Analyzer** page.

#### Task 5: Analyze mail flow

1. On Holly's **Mail** tab in the Microsoft Office 365 portal, click the **Apps** launcher in the top task bar, and click **Admin.**
2. In the Office 365 admin center, click **Admin centers**, click **Exchange**, and then click **mail flow**.
3. In **mail flow**, click **message trace**.
4. In **message trace**, next to Sender, click **add sender**.
5. In the **Select Members** dialog box, click **Holly**, click **add**, and then click **OK**.
6. Under Date range, select **Past 24 hours**.
7. Under Delivery status, select **Failed**, and then click **search**. Note the two messages.
8. Double-click each message to view the sender, recipient, message size, ID, and IP address information.
9. Note the differences between the message processing events: Receive, Submit, Spam Diagnostics, and Fail for the nonexistent domain, and Submit, Receive, Spam Diagnostics, and Fail for the nonexistent user.
10. Close the Message Trace window.

**Result**: After completing this exercise, you should have used the Message Header Analyzer to identify why email failed to deliver.

## Exercise 2: Monitoring service health and analyzing reports

#### Task 1: View Office 365 service health

1. In the Office 365 admin center, click **Home**.
2. On the **Home** page, in the left menu, select **Health**, and then click **Service health**.
3. Click **Go to the v2 Service Health page** link.
4. Select **Exchange Online** in the left column.
5. On the right side of the page, click **View history**.
6. Click any entry in the calendar that is colored yellow to see further details about incident. Details appear below the calendar.
7. Click the **Home** icon on the menu to the left.

#### Task 2: View reports in the Office 365 admin center

1. In the Office 365 admin center, on the **Home** page
2. In the menu to the left, click **REPORTS**, click **Usage**, and click **Email activity**.

**Note:** There might be little or no data shown because there is not much mailbox usage in the lab environment.

1. In the menu to the left, under **REPORTS**, click **Security & Compliance**
2. On the **Security & Compliance** page, in the **Protection** section, click **Sent and received mail**, and then click **View table**.
3. Close the table view.

**Note:** There might be little or no data shown because there is not much mailbox usage in the lab environment.

1. Close the open **Sent and received mail** window.
2. On the **Security & Compliance** page, in the Protection section, click **Malware detections**.
3. Close the open window.
4. On the **Security & Compliance** page, in the Protection section, click **Spam detections**.
5. Close the open window.
6. Keep the virtual machines running for the next lab.

**Result**: After completing this exercise, you should have monitored the health of Office 365 services and viewed reports in the Office 365 admin center.

©2016 Microsoft Corporation. All rights reserved.

The text in this document is available under the [Creative Commons Attribution 3.0 License](https://creativecommons.org/licenses/by/3.0/legalcode), additional terms may apply. All other content contained in this document (including, without limitation, trademarks, logos, images, etc.) are **not** included within the Creative Commons license grant. This document does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use this document for your internal, reference purposes.

This document is provided "as-is." Information and views expressed in this document, including URL and other Internet Web site references, may change without notice. You bear the risk of using it. Some examples are for illustration only and are fictitious. No real association is intended or inferred. Microsoft makes no warranties, express or implied, with respect to the information provided here.