Microsoft

O365 Supplemental Management Pack

Advanced O365 Monitoring using SCOM

Prepared for

10/3/2017

Version 1 Final

Created by

Taylour Blackwell and Brian Zoucha

Taylour.Blackwell@microsoft.com;

Brianz@microsoft.com

Microsoft

Contents

Microsoft

Overview

The Office 365 Supplemental Management Pack includes synthetic transactions that provide an increased level of visibility into the health of the Office 365 environment. For customers that don't have a monitoring solution they are limited to using the Admin Portal. We are providing this supplemental Management Pack for our customers leveraging System Center Operations Manager as their monitoring platform. There is a Management Pack available for Office 365, this management pack provides a deeper view into the health of the environment. The following Office 365 components are monitored using this supplemental management pack:

- Mail flow – Validate mail flow by sending a test email from a sender mailbox and validating receipt in the receiver mailbox.
- Licensing – Verification that a single user can obtain a license, Monitoring the available pool of licenses for a given subscription.

The management pack will execute these synthetic transactions from a local point-of-presence within the customer network for a comprehensive view of service availability.

Microsoft

Prerequisites and Requirements

The O365 Supplemental Management pack requires a working SCOM environment as a base.

The solution consists of the following elements added to the SCOM environment:

Management Pack

- **O365 Supplemental.mp**: Current version 1.311.4.9

Support Files

- **Exchange Web Services**: EWS is used to perform all mail flow workflows within the management pack.
- **Microsoft Online Services Sign-In Assistant for IT Professionals**: MOS SIA is used to login to Azure with PowerShell for the licensing workflows.
- **Windows Azure Active Directory PowerShell Module**: The Azure AD PowerShell module is used to run PowerShell scripts for the licensing tests.

Service Accounts

This solution utilizes SCOM's "RunAs" accounts to define credentials stored in SCOM and use them to execute the scripts within the workflows. A set of service accounts is required for on-premises and O365 based monitoring workflows.

- **On-Premises Workflows**
  - An Exchange username and password for *sending* email
  - An Exchange username and password for *receiving* email
- **O365 Workflows**
  - An Office 365 username and password for *sending* email
  - An Office 365 username and password for *receiving* email

Watcher Node

- This Management Pack solution requires at least one agent managed to computer to perform the workflows.

Microsoft

Watcher Node Preparation

The O365 Supplemental Management Pack requires watcher nodes with the SCOM agent installed to perform synthetic transactions and transmit results back to the management servers. These watcher nodes will need to have the prerequisite components installed for the synthetic transactions to work. Once you have located computers to work as watcher nodes you will need to make sure all the components below are installed on every watcher node.

- **SCOM Agent:** This SCOM agent needs to be a member of the SCOM management group that the O365 Supplemental MP is imported on.
- **Exchange Web Services**: Install EWS 2.2 from the following link on the server(s) that will run the mail flow synthetic test workflows: https://www.microsoft.com/en-us/download/details.aspx?id=42951
- **Microsoft Online Services Sign-In Assistant for IT Professionals**: Install on the server(s) that will run the licensing workflows. https://www.microsoft.com/en-us/download/details.aspx?id=41950
- **Windows Azure Active Directory PowerShell Module**: Install the azure PowerShell module on the server(s) that will run the licensing workflows. http://connect.microsoft.com/site1164/Downloads/DownloadDetails.aspx?DownloadID=59185

Microsoft

Management Pack Configuration

The steps below walk through the process to import and configure the O365 Supplemental Management pack into Operations Manager.

Deploy the O365 Supplemental management pack

Import the O365Supplemental.mp management pack using the steps below.

1. Log on to the computer with an account that is a member of the Operations Manager Administrators role for the Operations Manager management group.
2. In the Operations console, click **Administration**.
3. Right-click the **Management Packs** node, and then click **Import Management Packs**.
4. The **Import Management Packs** wizard opens. Click **Add**, and then click **Add from disk**.
5. The **Select Management Packs to import** dialog box appears. If necessary, change to the directory that holds your management pack file. Click the O365 Supplemental management pack to import from that directory, and then click **Open**.
6. On the **Select Management Packs** page, the management packs that you selected for import are listed. An icon next to each management pack in the list indicates the status of the selection, click **Import**.
7. The **Import Management Packs** page appears and shows the progress for each management pack. Each management pack is downloaded to a temporary directory, imported to Operations Manager, and then deleted from the temporary directory. If there is a problem at any stage of the import process, select the management pack in the list to view the status details. Click **Close**.

Creating a new Management Pack for customizations

The O365 Supplemental management pack is sealed so that you cannot change any of the original settings in the management pack file. However, you can create customizations, such as overrides or new monitoring objects, and save them to a different management pack. By default, the Operations Manager saves all customizations to the default management pack. As a best practice, you should instead create a separate management pack for each sealed management pack you want to customize.

1. Open the **Operations Manager** console, and then click **Administration** button.
2. Right-click **Management Packs**, and then click **Create New Management Pack**.
3. Enter a name (for example, **O365 Supplemental Overrides**), and then click **Next**.
4. Click **Create**.

Create a RunAs Accounts

The O365 Supplemental management pack utilizes RunAs Accounts to perform workflows to test the O365 environment. Run As accounts will need to be configured for all the Run As profiles. **Note**: You will need to logon and connect to the Operations Manager console with an account that is a member of the Operations Manager Administrators role to complete the following operations.

- O365 Sender Profile
- O365 Receiver Profile
- Exchange Sender Profile
- Exchange Receiver Profile
- License Verification Profile

1. In the Operations console, click **Administration**.
2. In the Administration pane, expand **Administration**, expand **RunAs Configuration**, right-click **Accounts**, and then click **Create RunAs Account…**.
3. In the **Create RunAs Account Wizard**, on the **Introduction** page click **Next.**
4. On the **General Properties** page, do the following:
    1. Select **Windows** in the **RunAs Account type:** list.
    2. Type a display name in the **Display Name** text box,
    3. Optionally, type a description in the **Description** box.
    4. Click **Next**.
5. On the **Credentials** page, type a username (Must use the format Username@domain.com), and its password, for the account that you want to use with this **RunAs Account**.
6. Click **Next**.
7. On the **Distribution Security** page, select the **More secure** option as appropriate.
8. Click **Create**.
9. On the **RunAs Account Creation Progress** page, click **Close**.

Configuring RunAs Profiles

Pre-existing Run As profiles have been created when the O365 Supplemental management pack was imported. Use this procedure to modify the properties of Run As profiles to use the RunAs Accounts created above. **Note**: You will need to logon and connect to the Operations Manager console with an account that is a member of the Operations Manager Administrators role to complete the following operations.

1. Select the **Administration** view.
2. In the **Administration** view navigation pane, select the **Profiles** container.
3. In the results pane, double-click the profile whose properties you want to edit. This opens the **Run As Profile Wizard**, which contains the settings that were configured previously.
4. On the **General Properties** page, you can modify the value in the **Display name** and **Description** fields.
5. Click **Next**.
6. On the **Run As Accounts** page, you can add additional Run As accounts, edit the settings of existing ones and remove Run As accounts that should no longer be associated with the Run As profile.
7. When you have completed your modifications, click **Save**.
8. On the **Completion** page, in the **More-secure Run As accounts:** box, you must select each account in turn and configure the distribution of the credentials for each Run As account.
9. When you have completed configuring distribution, click **Close**.

Enable and Configure Monitors

You will need to override monitors and rules to for the workflows you intend to use in order to enable monitoring utilizing the synthetic transaction scripts on watcher machines. The steps below will walk you through the process of enabling and setting parameters through overrides for each monitor included in the management pack.

O365 to O365 Mail Flow Monitor

This monitor utilizes synthetic transactions to verify the flow of email from an O365 email account to another O365 email account. This monitor has two health states, healthy and critical. The health state is determined if the synthetic transaction is or is not able to successfully complete for any reason. The synthetic transaction works by logging into a sender account using the "O365 Sender Profile" and sending a test email to the receiver account specified in the "O365 Receiver Profile". The monitor then logs into the receiver account using the "O365 Receiver Profile" to verify the test email was received.

This monitor contains the following overridable parameters.		
Parameter	Default Value	Details

This monitor contains the following overridable parameters.		
Script Timeout	300 Sec	This set the amount of time the synthetic transaction must complete before it errors out. The default value can be left or can be adjusted to fit the environment.
Interval Seconds	900 Sec	This sets how long the monitor waits until running the synthetic transaction again. The default value can be left or can be adjusted to fit the environment.
Enabled*	False	This needs to be overridden and set to True for all watcher nodes. This allows the monitor to run the synthetic transaction workflows.
O365 URL*	None	This needs to be overridden and populated with the URL for the O365 EWS URL utilized in your environment.
Sleep Int	5 Sec	This value determines how long the monitor waits between search attempts during each run of the synthetic transaction. The synthetic transaction will attempt to search for the received email 10 times. The default value can be left or can be adjusted to fit the environment.

1. In the Operations console, click the **Authoring** button.
2. In the **Authoring** pane, expand **Management Pack Objects** and then click **Monitors**.
3. On the toolbar, click **Scope**.
4. In the **Scope Management Pack Target(s) by object** dialog box, in the **Look for** box, type "O356 Watcher".
5. Click the check box next to **O365 Watcher Node**.
6. Click **OK** to close the dialog box.
7. After the monitors have loaded, click **O365 Watcher Node** > **Entity Health** > **Availability> Office 365 Supplemental MP WatcherNode Aggregate Monitor Availability**.
8. Under **Availability**, right-click the rule **O365 to O365 Mail Flow Monitor**, and then click **Overrides** > **Override the Monitor** > **For a specific object of the Class: O365 watcher Node**.
9. In the **Select Object dialog** box, select the watcher node, and then click **OK**.
10. In the **Override Properties** dialog box, select the **Override** check box next to **Enabled**.
11. Set the override value to **True**.
12. In the **Override Properties** dialog box, select the **Override** check box next to **O365 URL**.

13. Set the override value to the O365 EWS URL.
14. Click **OK**

O365 to Exchange Mail Flow Monitor

This monitor utilizes synthetic transactions to verify the flow of email from an O365 email account to an Exchange email account. This monitor has two health states, healthy and critical. The health state is determined if the synthetic transaction is or is not able to successfully complete for any reason. The synthetic transaction works by logging into a sender account using the "O365 Sender Profile" and sending a test email to the receiver account specified in the "Exchange Receiver Profile". The monitor then logs into the receiver account using the "Exchange Receiver Profile" to verify the test email was received.

This monitor contains the following overridable parameters.		
Parameter	Default Value	Details
Script Timeout	300 Sec	This set the amount of time the synthetic transaction must complete before it errors out. The default value can be left or can be adjusted to fit the environment.
Interval Seconds	900 Sec	This sets how long the monitor waits until running the synthetic transaction again. The default value can be left or can be adjusted to fit the environment.
Enabled*	False	This needs to be overridden and set to true for all watcher nodes. This allows the monitor to run the synthetic transaction workflows.
O365 URL*	None	This needs to be overridden and populated with the URL for the O365 EWS URL utilized in your environment.
Exchange URL*	None	This needs to be overridden and populated with the URL for the Exchange EWS URL utilized in your environment.
SleepInt	5 Sec	This value determines how long the monitor waits between search attempts during each run of the synthetic transaction. The synthetic transaction will attempt to search for the received email 10 times. The default value can be left or can be adjusted to fit the environment.

1. In the Operations console, click the **Authoring** button.
2. In the **Authoring** pane, expand **Management Pack Objects** and then click **Monitors**.
3. On the toolbar, click **Scope**.
4. In the **Scope Management Pack Target(s) by object** dialog box, in the **Look for** box, type "O365 Watcher".
5. Click the check box next to **O365 Watcher Node**.
6. Click **OK** to close the dialog box.
7. After the monitors have loaded, click **O365 Watcher Node**> **Entity Health** > **Availability> Office 365 Supplemental MP WatcherNode Aggregate Monitor Availability**.
8. Under **Availability**, right-click the rule **O365 to Exchange Mail Flow Monitor**, and then click **Overrides** > **Override the Monitor** > **For a specific object of the Class: O365 Watcher Node**.
9. In the **Select Object dialog** box, select the watcher node, and then click **OK**.
10. In the **Override Properties** dialog box, select the **Override** check box next to **Enabled**.
11. Set the override value to **True**.
12. In the Override Properties dialog box, select the Override check box next to O365 URL.
13. Set the override value to the O365 EWS URL.
14. In the **Override Properties** dialog box, select the **Override** check box next to **Exchange URL**.
15. Set the override value to the Exchange EWS URL.
16. Click **OK**

Exchange to O365 Mail Flow Monitor

This monitor utilizes synthetic transactions to verify the flow of email from an Exchange email account to an O365 email account. This monitor has two health states, healthy and critical. The health state is determined if the synthetic transaction is or is not able to successfully complete for any reason. The synthetic transaction works by logging into a sender account using the "Exchange Sender Profile" and sending a test email to the receiver account specified in the "O365 Receiver Profile". The monitor then logs into the receiver account using the "O365 Receiver Profile" to verify the test email was received.

This monitor contains the following overridable parameters.		
Parameter	Default Value	Details
Script Timeout	300 Sec	This set the amount of time the synthetic transaction must complete before it errors out. The default value can be left or can be adjusted to fit the environment.
Interval Seconds	900 Sec	This sets how long the monitor waits until running the synthetic transaction again. The default value can be left or can be adjusted to fit the environment.
Enabled	False	This need to be overridden and set to True for all watcher nodes. This allows the monitor to run the synthetic transaction workflows.
O365 URL*	None	This needs to be overridden and populated with the URL for the O365 EWS URL utilized in your environment.
Exchange URL*	None	This needs to be overridden and populated with the URL for the Exchange EWS URL utilized in your environment.
Sleep Int	5 Sec	This value determines how long the monitor waits between search attempts during each run of the synthetic transaction. The synthetic transaction will attempt to search for the received email 10 times. The default value can be left or can be adjusted to fit the environment.

1. In the Operations console, click the **Authoring** button.
2. In the **Authoring** pane, expand **Management Pack Objects** and then click **Monitors**.
3. On the toolbar, click **Scope**.
4. In the **Scope Management Pack Target(s) by object** dialog box, in the **Look for** box, type "O365 Watcher".
5. Click the check box next to **O365 Watcher Node**.
6. Click **OK** to close the dialog box.
7. After the monitors have loaded, click **O365 Watcher Node**> **Entity Health** > **Availability**> **Office 365 Supplemental MP Watcher Node Aggregate Monitor Availability**.
8. Under **Availability**, right-click the rule **Exchange to O365 Mail Flow Monitor**, and then click **Overrides** > **Override the Monitor** > **For a specific object of the Class: O365 Watcher Node**.

9. In the **Select Object dialog** box, select the watcher node, and then click **OK**.
10. In the **Override Properties** dialog box, select the **Override** check box next to **Enabled**.
11. Set the override value to **True**.
12. In the **Override Properties** dialog box, select the **Override** check box next to **O365 URL**.
13. Set the override value to the O365 EWS URL.
14. In the **Override Properties** dialog box, select the **Override** check box next to **Exchange URL**.
15. Set the override value to the Exchange EWS URL.
16. Click **OK**

O365 Available License Monitor

This monitor utilizes Azure Active Directory PowerShell Module to verify that number of available licenses for a particular SKU is greater than the set threshold. The "License Verification Profile" is used to run the workflow. This monitor has three health states, healthy, warning and critical. The health state is determined by running the **Get-MsolAccountSku** and then we need to make sure we actually have a license to assign. To determine that, we take the value of **ActiveUnits** property (25) and subtract the value of the **ConsumedUnits** (24) property:

25 - 24 = 1

The **ActiveUnits** property tells us how many licenses we've purchased, and the value **ConsumedUnits** tells us how many licenses are currently in use. If we subtract the number of licenses already spoken for from the number of licenses we purchased, we'll know how many licenses are still available.

This monitor contains the following overridable parameters.		
Parameter	Default Value	Details
Script Timeout	300 Sec	This set the amount of time the synthetic transaction must complete before it errors out. The default value can be left or can be adjusted to fit the environment.
Interval Seconds	900 Sec	This sets how long the monitor waits until running the synthetic transaction again. The default value can be left or can be adjusted to fit the environment.

This monitor contains the following overridable parameters.		
Enabled*	False	This needs to be overridden and set to True for all watcher nodes. This allows the monitor to run the synthetic transaction workflows.
Rem Licenses Error	5	This sets the critical alert threshold for the monitor if the number of available licenses is less the set value it will cause an alert to be generated. The default value can be left or can be adjusted to fit the environment.
Rem Licenses Warn	10	This sets the warning alert threshold for the monitor if the number of available licenses is less the set value it will cause an alert to be generated. The default value can be left or can be adjusted to fit the environment.
Sku Type*	None	This need to be overridden to the account sku you wish to monitor on all watcher nodes. The available SKUs for your environment can be found by running the Get Account SKU Task.

1. Log on to the computer with an account that is a member of the Operations Manager Advanced Operator role for the Operations Manager management group.
2. In the Operations console, click the **Authoring** button.
3. In the **Authoring** pane, expand **Management Pack Objects** and then click **Monitors**.
4. On the toolbar, click **Scope**.
5. In the **Scope Management Pack Target(s) by object** dialog box, in the **Look for** box, type "O365 Watcher".
6. Click the check box next to **O365 Watcher Node**.
7. Click **OK** to close the dialog box.
8. After the monitors have loaded, click **O365 Watcher Node**> **Entity Health** > **Availability**> **Office 365 Supplemental MP WatcherNode Aggregate Monitor Availability**.
9. Under **Availability**, right-click the rule **O365 Available License Monitor**, and then click **Overrides** > **Override the Monitor** > **For a specific object of the Class: O365 Watcher Node**.
10. In the **Select Object dialog** box, select the watcher node, and then click **OK**.
11. In the **Override Properties** dialog box, select the **Override** check box next to **Enabled**.
12. Set the override value to **True**.

13. In the **Override Properties** dialog box, select the **Override** check box next to **RemLicenses**.
14. Set the override value to **License Threshold** (any number you choose).
15. In the **Override Properties** dialog box, select the **Override** check box next to **SkuType**.
16. Set the override value to **Monitored Sku Type**.
17. Click **OK**

O365 Office Pro Plus License Verification Monitor

This monitor utilizes Azure Active Directory PowerShell Module to verify that user specified in the "License Verification Profile" is able to obtain a license. This monitor has two health states, healthy and critical. The health state is simply determined by whether a license is obtained.

This monitor contains the following overridable parameters.		
Parameter	Default Value	Details
Script Timeout	300 Sec	This set the amount of time the synthetic transaction must complete before it errors out. The default value can be left or can be adjusted to fit the environment.
Interval Seconds	900 Sec	This sets how long the monitor waits until running the synthetic transaction again. The default value can be left or can be adjusted to fit the environment.
Enabled	False	This need to be overridden to true for all watcher nodes. This allows the monitor to run the synthetic transaction workflows.

1. In the Operations console, click the **Authoring** button.
2. In the **Authoring** pane, expand **Management Pack Objects** and then click **Monitors**.
3. On the toolbar, click **Scope**.
4. In the **Scope Management Pack Target(s) by object** dialog box, in the **Look for** box, type "O365 Watcher".
5. Click the check box next to **O365 Watcher Node**.
6. Click **OK** to close the dialog box.
7. After the monitors have loaded, click **O365 Watcher Node**> **Entity Health** > **Availability**> **Office 365 Supplemental MP WatcherNode Aggregate Monitor Availability**.

8. Under **Availability**, right-click the rule **O365 Office Pro Plus License Verification Monitor**, and then click **Overrides** > **Override the Monitor** > **For a specific object of the Class: O365 Watcher Node**.
9. In the **Select Object dialog** box, select the watcher node, and then click **OK**.
10. In the **Override Properties** dialog box, select the **Override** check box next to **Enabled**.
11. Set the override value to **True**.
12. Click **OK**

Microsoft

Management Pack Overview

This solution is powered by a custom management pack consisting of multiple workflows and run as profiles to monitor mail flow and licensing. This provides additional insight regarding the health of an organizations email infrastructure.

Monitors

- **O365 to O365 Mail Flow Monitor**
  - This monitor logs into O365 using the O365 Sender Profile and sends a test message to the O365 Receiver Profile. It then logs into the account specified in the O365 Receiver Profile and verifies receipt of the email from the O365 Sender Profile.
- **Exchange to O365 Mail Flow Monitor**
  - This monitor logs into Exchange using the Exchange Sender Profile and sends a test message to the O365 Receiver Profile. It then logs into the account specified in the O365 Receiver Profile and verifies receipt of the email from the Exchange Sender Profile.
- **O365 to Exchange Mail Flow Monitor**
  - This monitor logs into O365 using the O365 Sender Profile and sends a test message to the Exchange Receiver Profile. It then logs into the account specified in the Exchange Receiver Profile and verifies receipt of the email from the O365 Sender Profile.
- **O365 Office Pro Plus License Verification Monitor**
  - This monitor uses PowerShell to determine if there are O365 licenses available and a connection can be made to retrieve licenses.
- **O365 Available License Count Monitor**
  - This monitor uses PowerShell to determine if the number of available of O365 licenses is greater than the set threshold.

Rules

- **O365 to O365 Mail Flow Event Collection**
  - This rule looks for and collects the event ID 40 in the Operations Manager log.
- **O365 to Exchange Mail Flow Event Collection**
  - This rule looks for and collects the event ID 43 in the Operations Manager log.
- **Exchange to O365 Mail Flow Event Collection**
  - This rule looks for and collects the event ID 42 in the Operations manager log.
- **O365 Office Pro Plus License Verification Event Collection**
  - This rule looks for and collects the event 41 ID in the Operations Manager Log.
- **O365 Office Pro Plus License Verification Event Collection**
  - This rule looks for and collects the event 44 ID in the Operations Manager Log.

Run as Profiles

When the O365 Supplemental Management Pack is imported for the first time, it creates five new Run As profiles:

- **Office 365 Supplemental O365 Sender Profile**
  - This profile is used to login and send email using O365.
- **Office 365 Supplemental O365 Receiver Profile**
  - This profile is used to login and receive email using O365.
- **Office 365 Supplemental Exchange Sender Profile**
  - This profile is used to login and send email using exchange.
- **Office 365 Supplemental Exchange Receiver Profile**
  - This profile is used to login and receive email using exchange.
- **Office 365 Supplemental License Verification Profile**
  - This profile is used to verify O365 Licensing information.

Tasks

- **Get Account Sku**
  - This task outputs the SKUs associated with the license verification profile.
- **O365 SMP Prerequisite Verification**
  - This task outputs the install status of prerequisites required on watcher nodes.

Dashboards

- **O365 Mail Flow Dashboard**
  - This dashboard displays all mail flow related alerts and events for the O365 Supplemental MP.
- **O365 Licensing Dashboard**
  - This dashboard displays all licensing related alerts and events for the O365 Supplemental MP.