# A close up of a sign Description automatically generatedMicrosoft Windows Virtual Desktop – Monitoring Setup

Information in this document, including URL and other Internet Web site references, is subject to change without notice. Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, e-mail address, logo, person, place or event is intended or should be inferred. Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

The names of manufacturers, products, or URLs are provided for informational purposes only and Microsoft makes no representations and warranties, either expressed, implied, or statutory, regarding these manufacturers or the use of the products with any Microsoft technologies. The inclusion of a manufacturer or product does not imply endorsement of Microsoft of the manufacturer or product. Links may be provided to third party sites. Such sites are not under the control of Microsoft and Microsoft is not responsible for the contents of any linked site or any link contained in a linked site, or any changes or updates to such sites. Microsoft is not responsible for webcasting or any other form of transmission received from any linked site. Microsoft is providing these links to you only as a convenience, and the inclusion of any link does not imply endorsement of Microsoft of the site or the products contained therein.

© 2019 Microsoft Corporation. All rights reserved.

Microsoft and the trademarks listed at <https://www.microsoft.com/en-us/legal/intellectualproperty/Trademarks/Usage/General.aspx> are trademarks of the Microsoft group of companies. All other trademarks are property of their respective owners.

Contents

[Microsoft Windows Virtual Desktop – Monitoring Setup 1](#_Toc22037631)

[WVD Monitoring 4](#_Toc22037632)

[Task 1: Installation for a new Log Analytics Workspace 5](#_Toc22037633)

[Task 2: Installation for an already existing Log Analytics Workspace 6](#_Toc22037634)

[Task 3: Sepago Agent Installation 6](#_Toc22037635)

[Task 4: Windows Virtual Desktop Service Tenant Diagnostic injection – Log Analytics 10](#_Toc22037636)

[Task 5: Log Analytics Interdependency Agent Metrics 11](#_Toc22037637)

## WVD Monitoring

The following describes the process for you to set up [monitoring](http://loganalytics.sepago.com/index.html) for your WVD environment. This solution uses a 3rd party partner available in our Azure Gallery. This is referred to as a ‘Microsoft Preferred Solution’. A Microsoft preferred solution is a cloud application selected for its quality, performance, and ability to address customer needs in a certain industry vertical or solution area. A team of Microsoft experts validates solutions from partners with specific proven competencies and capabilities. These solutions are featured in our cloud marketplace storefronts, Azure Marketplace, and AppSource, as well as in the Azure portal. Preferred solutions on AppSource can be discovered by industry verticals. Preferred solutions on Azure Marketplace and the Azure portal can be discovered across horizontal solution categories.

The Sepago Agent monitors each worker in your RDS or Citrix environment. The agent is focused on events, performance consumption, network activities and more regarding each user’s IT experiences. Workers in this context are Windows Remote Desktop Server or Windows 10\MS, XenApp Servers and of course Windows Client VDI’s (XenDesktop). The agents combine data from different sources and send them to your OMS Log Analytics workspace in Azure.

A screenshot of a cell phone

Description automatically generated

#### Task 1: Installation for a new Log Analytics Workspace

From the Azure Portal, you select create a resource and search for Azure Monitor for RDS and Windows Virtual Desktop. Make sure you deploy the workspace in **East US as that is where you can leverage the Interdependency agent** to show application and port mappings to your servers.

A screenshot of a social media post

Description automatically generated

Click Create and run through the steps:

A screenshot of a cell phone

Description automatically generated

#### Task 2: Installation for an already existing Log Analytics Workspace

If you want to leverage an already existing Log Analytics workspace in **EAST US**, then all you need to do is import the views which can be downloaded from here, [https://github.com/hardeights/wvd/tree/master/WVD%20Monitoring/](https://github.com/hardeights/wvd/tree/master/WVD%20Monitoring/Views)Views . Open up Log Analytics workspace and in the middle blade select view designer. Click import and browse to the view files you downloaded.

A screenshot of a cell phone

Description automatically generated

A screenshot of a cell phone

Description automatically generated

#### Task 3: Sepago Agent Installation

Once you have the workspace created above or you are using a workspace already built you need to deploy the agents to all your session hosts and\or add the agent to a master image. You can grab the agent from [here](http://loganalytics.sepago.com/downloads/ITPC-LogAnalyticsAgent.zip). Once you have it downloaded and extracted you need to configure it for your Log Analytics Workspace. Find the file marked config at the end. Open it in notepad or what editor you like. Change the two key values “Customer ID and Shared Key”.

A screenshot of a cell phone

Description automatically generated

|  |  |
| --- | --- |
| Customer ID: Workspace ID  Shared Key: Primary Key | A screenshot of a social media post  Description automatically generated |

A screenshot of a cell phone

Description automatically generated

Open a cmd window as administrator. Change directory to where the agent has been copied.   
ITPC-LogAnalyticsAgent.exe -test

If you see the below output stating “error” there is a potential communication problem , either the workspace ID or Key is incorrect or the session host can’t communicate to the LA Workspace due to networking.

A screenshot of a cell phone

Description automatically generated

If all is configured correctly, you should see the below output.

A screenshot of a cell phone

Description automatically generated  
  
Make sure all is working as expected. If it is, then execute this command,   
ITPC-LogAnalyticsAgent.exe -install

A screen shot of a computer

Description automatically generated

If you look at the task scheduler you should see the below:

A screenshot of a cell phone

Description automatically generated

The time it takes to see data varies, but in my experience its about 24-36 hours.

You can then publish a new dashboard for example below:

A screenshot of a cell phone

Description automatically generated

#### Task 4: Windows Virtual Desktop Service Tenant Diagnostic injection – Log Analytics

Taking your Log Analytics workspace ID and primary key, you can apply this to your Windows Virtual Desktop Tenant(s) by following the below. Open PowerShell with an elevated account.

Import-module Microsoft.RDInfra.RDPowershell.dll  
  
Add-RDSAccount -DeploymentUrl https://rdbroker.wvd.microsoft.com

Set-RdsTenant -Name "jojenner" -LogAnalyticsWorkspaceId "96f3255d-547f-XXf4-XXXX-fef7e" -LogAnalyticsPrimaryKey "sBNWCfjb92E19dYHcGsX||||||k0aDPUP3NOogrZC8QoTwV+ZBQ99dhf3K0XXXXo1Mu3eZExEyZXW4fB="

PS C:\WINDOWS\system32> get-rdstenant "jojenner"

TenantGroupName : Default Tenant Group

AadTenantId : XXXXXXXX

Description : John Jenner WVD Environment

FriendlyName :

SsoAdfsAuthority :

SsoClientId :

SsoClientSecret :

AzureSubscriptionId :

LogAnalyticsWorkspaceId : 96f3255d-547f-XXXX-9a55-fef7e19808bc

LogAnalyticsPrimaryKey : \*\*\*\*\*\*\*\*

Login a few times to your session hosts and click some applications. Try and login with an account you know does not have permissions as well. Browse to your log analytics workspace and look for logs in the middle blade. Expand the tree under ‘custom logs’ and you should see something like the below: WVDActivityV1, WVDCheckpointV1 and WVDErrorV1.   
  
A screenshot of a cell phone

Description automatically generated

A screenshot of a cell phone

Description automatically generated

The other ITPC ones listed are from the above steps (Sepago). If you have followed this document fully, you should see similar items to what is above in custom logs providing you have errors in WVD to report into this log (WVDErrorV1\_CL).

#### Task 5: Log Analytics Interdependency Agent Metrics

The Map feature in Azure Monitor for VMs gets its data from the Microsoft Dependency agent. The Dependency agent relies on the Log Analytics agent for its connection to Log Analytics. Your system must have the Log Analytics agent installed and configured with the Dependency agent.

Whether you enable Azure Monitor for VMs for a single Azure VM or you use the at-scale deployment method, use the Azure VM Dependency agent extension to install the agent as part of the experience.

Once you install this agent on your session hosts or golden image, you can then show the below data to your clients by going to the virtual machine object, and in the middle blade selecting ‘insights’.  
  
A screenshot of a cell phone

Description automatically generated

Once you click ‘insights’ a menu on the right will show,   
A screenshot of a cell phone

Description automatically generated

It is the MAP we are interested in for this exercise. You can also use the other 2 options to show value add (Performance and Health)

A close up of a map

Description automatically generated

In the middle we can see the processes running on our session host and where they are communicating to.

Port 443, these are all outbound calls from your session host (wvd-poolapp-0)

If you click the top right box,  
For example, network dependencies will show you these options

A screenshot of a cell phone

Description automatically generated

A screenshot of a cell phone

Description automatically generated

Click the active ports for example and you will see the below data,

A screenshot of a cell phone

Description automatically generated