Make the Invisible Visible™



Improve the security of an ICONICS Virtual Machine from Azure Marketplace

An ICONICS Whitepaper

June 2020

Version 1.0

Contents

1 Introduction 4
2 Securing the ICONICS virtual machine network security group(NSG) rules 4
3 Securing SQL Server access 5
4 Conclusion 7

© 2020 ICONICS, Inc. All rights reserved

Copyright and Confidentiality

By accessing and using the installation instructions (the “instructions”) you acknowledge and agree, on your behalf and on behalf of the person, entity or other organization on whose behalf you are accessing the instructions, that neither ICONICS nor any of its service providers, including, without limitation, any system integrator or independent software vendor: (1) makes any representations or warranties of any kind, either express, implied, statuary or otherwise with respect to the instructions, including the accuracy, completeness or usefulness thereof; and (2) shall be liable for damages of any kind, under any legal theory, arising out of or in connection with your election to follow or use, or inability to follow or use, the instructions, including any direct, indirect, incidental, special, punitive or consequential damages, or for loss of use, loss of profits, loss of data, loss of business, or loss of privacy or security, even if foreseeable, arising out of or in connection with your election to follow or use, or inability to follow or use, the instructions. You further acknowledge and agree that your use of the instructions, whether directly or indirectly, is at your own risk and that you expressly assume all risk in connection with your use of the instructions. If you do not agree to the foregoing, you may not access or use the instructions.

Copyright © 2020, ICONICS, Inc. All rights reserved.

Authors

- Zhi Wei Li, Director of Innovation and Incubation Solutions

 © 2020 ICONICS, Inc. All rights reserved

1 Introduction

With the availability of ICONICS' virtual machine offers on the Azure Marketplace, it is now incredibly easy and quick to create an ICONICS environment on Microsoft Azure.

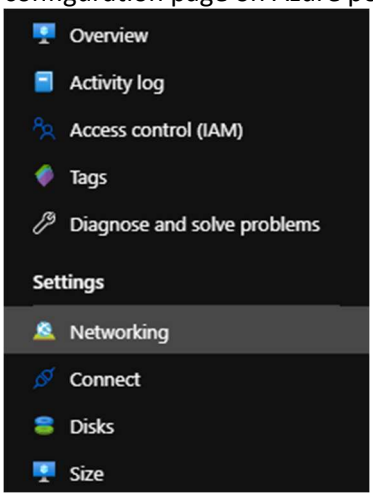
However, for applications that require an elevated security posture, this whitepaper outlines the recommended steps to take, post-deployment, to improve the security posture of the ICONICS environment.

2 Securing the ICONICS virtual machine network security group(NSG) rules

When a virtual machine is provisioned using one of the ICONICS offers on Azure Marketplace, a set of pre-defined network security group (NSG) rules are applied. These rules are meant to allow users to easily access the various ICONICS capabilities without any post deployment steps.

To improve the security posture of the virtual machine, these NSG rules should be reviewed and modified as necessary.

The NSG rules can be accessed by clicking on the Networking setting of the virtual machine configuration page on Azure portal:



As part of the marketplace offer, the following ports are allowed for inbound communication:

- TCP 8778
    - This port is allowed to facilitate ICONICS FrameWorX communication between ICONICS servers
    - While this port is allowed at the NSG level, it is not allowed in the Windows Firewall settings of the virtual machine
    - Remove this port from the NSG rules if your ICONICS virtual machine is not expected to be a data source to other ICONICS servers

© 2020 ICONICS, Inc. All rights reserved

- TCP 80
    - This port is allowed to facilitate http communication to access ICONICS web front ends
    - For production use cases, it is recommended to use the encrypted https communication channel with a certificate authority issued SSL certificate
    - Remove this port from the NSG rules if https communication is enabled
- TCP 443
    - This port is allowed to facilitate https communication to access ICONICS web front ends
    - Remove this port from the NSG rules if https communication will not be used
      NOTE: It is strongly recommended that for production uses, https communication with a certificate authority issued SSL certificate be used instead of http
- TCP 3389
    - This port is allowed to facilitate remote desktop access to the virtual machine
    - It is recommended to modify this NSG rule to limit the source IP ranges only to trusted IP addresses. To do so, follow the steps below:
        a. Click on the **default-allow-rdp** NSG rule
        b. In the settings blade that shows up to the right, click on the **Source** drop down
        c. Select **IP Addresses**
        d. Enter the **Source IP addresses** or **CIDR ranges** for your list of trusted IPs
        e. Click **Save** at the top
        f. Once applied, only IP addresses that are allowed can remote desktop to the virtual machine

3 Securing SQL Server access

When a virtual machine is provisioned using one of the ICONICS offers on Azure Marketplace, it comes pre-installed with the edition of SQL server that ships with the respective ICONICS Suite version. The SQL server is setup in a specific way that allows for replication of the virtual machine and may not meet your desired security posture.

To improve the security posture of the provided SQL server, the following recommendations should be reviewed and taken if applicable.

- Update the pre-defined ICONICS_USER SQL account password
- Review your organization's IT policies to understand if SQL accounts are allowed.
- Review and lock down the users that have access to the SQL server

3.1 To update ICONICS_USER SQL account password, perform the following steps:

1. Update the ICONICS_USER SQL account password
    a. From the Start menu, expand the **Microsoft SQL Server Tools 18** folder
    b. Launch the **Microsoft SQL Server Management Studio**
    c. In the **Server name** field of the login dialog, enter **(local)**
    d. For the **Authentication** field of the login dialog, select **Windows Authentication**
    e. Click **Connect**
    f. From the **Object Explorer** pane, expand **Security → Logins**
    g. Right click on **iconics_user**
    h. Select **Properties**

© 2020 ICONICS, Inc. All rights reserved

i. Update the password in the **Password** and **Confirm password** field
j. Click **OK**

2. Update the ICONICS connection string information
    a. Launch Windows Explorer
    b. Go to **C:\Program Files\ICONICS\GENESIS64\Components**
    c. Launch **IcoWorkbenchInstaller.exe**
    d. Set the **SQL Server** as '**(local)**'
    e. Change **SQL Security** to **Use SQL Security**
    f. In the **SQL Server Username** field, enter **iconics_user**
    g. In the **SQL Server Password**, enter the updated password
    h. Uncheck **Enable Project Reporting**
    i. Click **Next**
    j. In the next dialog, under the **Configuration Settings** section
        i. Uncheck **Include samples in all configurations**
        ii. Uncheck **Overwrite all configurations**
    k. In the **Setup Configuration** section
        i. Uncheck **Overwrite** on the right
    l. Click on **Install**
    m. The update operation will execute
    n. You will see some warnings and errors towards the end of the operation. This is normal.
    o. Click **Continue** to close the dialog
    p. Reboot the virtual machine

3.2 To remove the use of SQL accounts, perform the following steps:

1. Update ICONICS configuration
    a. From the Start menu, expand the **ICONICS Tools** folder
    b. Launch **Configure System**
    c. In the **User Configuration** dialog, check off **Create New User** at the top left
    d. In the **Server or Domain** field, click on the **Browse** button next to it
    e. Select the local machine from the list that shows up and click **OK**
    f. In the **User Name** field, enter a new user name
    g. In the **Password** field, enter a desired strong password
    h. In the **Retype Password** field, repeat the chosen strong password
    i. Click **Next**
    j. In the ensuing Database and Services Setup dialog, for the **SQL Security** field, make sure **Use Windows NT Integrated Security** is chosen
    k. Uncheck **Enable Project Reporting**
    l. Click **Next**
    m. In the next dialog, under the **Configuration Settings** section
        i. Uncheck **Include samples in all configurations**
        ii. Uncheck **Overwrite all configurations**
    n. In the **Setup Configuration** section
        i. Uncheck **Overwrite** on the right
    o. Click on **Install**
    p. The update operation will execute
    q. Once the configuration steps are complete, click on Continue to close the dialog
    r. Reboot the virtual machine

© 2020 ICONICS, Inc. All rights reserved

2. Disable the use of SQL accounts
    a. From the Start menu, expand the **Microsoft SQL Server Tools 18** folder
    b. Launch the **Microsoft SQL Server Management Studio**
    c. In the **Server name** field of the login dialog, enter **(local)**
    d. For the **Authentication** field of the login dialog, select **Windows Authentication**
    e. Click **Connect**
    f. From the **Object Explorer** pane, right click on the **(local)** SQL server top level item
    g. Select **Properties**
    h. In the **Server Properties** dialog, select **Security**
    i. Under the **Server authentication** section, select the **Windows Authentication mode** radio button
    j. Click **OK**

3.3 To review and lock down SQL server access, perform the following steps:

1. From the Start menu, expand the **Microsoft SQL Server Tools 18** folder
2. Launch the **Microsoft SQL Server Management Studio**
3. In the **Server name** field of the login dialog, enter **(local)**
4. For the **Authentication** field of the login dialog, select **Windows Authentication**
5. Click **Connect**
6. From the **Object Explorer** pane, expand **Security → Logins**
7. Review the list of users and groups allowed to access SQL server
8. Remove any user or group that should not have access as per your organization's desired security posture
   NOTE: Ensure that the user used by ICONICS services to access configuration databases are still allowed

4 Conclusion

ICONICS based solutions can be rapidly deployed by leveraging the ICONICS offers on Azure Marketplace. Combined with the recommendations outlined in this whitepaper, the security posture of the solutions can be improved to better meet your organization's recommendations.

© 2020 ICONICS, Inc. All rights reserved



Founded in 1986, ICONICS is an award-winning independent software provider offering real-time visualization, HMI/SCADA, energy management, fault detection, manufacturing intelligence, MES, and a suite of analytics solutions for operational excellence. ICONICS solutions are installed in 70 percent of the Global 500 companies around the world, helping customers to be more profitable, agile and efficient, to improve quality, and to be more sustainable.

ICONICS is leading the way in cloud-based solutions with its HMI/SCADA, analytics, mobile and data historian to help its customers embrace the Internet of Things (IoT). ICONICS products are used in manufacturing, building automation, oil and gas, renewable energy, utilities, water and wastewater, pharmaceuticals, automotive, and many other industries. ICONICS' advanced visualization, productivity, and sustainability solutions are built on its flagship products: GENESIS64™ HMI/SCADA, Hyper Historian™ plant historian, AnalytiX® solution suite, and MobileHMI™ mobile apps. Delivering information anytime, anywhere, ICONICS' solutions scale from the smallest standalone embedded projects to the largest enterprise applications.

ICONICS promotes an international culture of innovation, creativity, and excellence in product design, development, technical support, training, sales, and consulting services for end users, systems integrators, OEMs, and channel partners. ICONICS has over 375,000 applications installed in multiple industries worldwide.

ICONICS Sales Offices

World Headquarters
100 Foxborough Blvd.
Foxborough, MA, USA, 02035
+1 508 543 8600
us@iconics.com

European Headquarters
Netherlands
+31 252 228 588
holland@iconics.com

Australia
+61 2 9605 1333
australia@iconics.com

Canada
+1 647 544 1150
canada@iconics.com

China
+86 10 8494 2570
china@iconics.com

Czech Republic
+420 377 183 420
czech@iconics.com

France
+33 4 50 19 11 80
france@iconics.com

Germany
+49 2241 16 508 0
germany@iconics.com

India
+91 265 6700821
india@iconics.com

Italy
+39 010 46 0626
italy@iconics.com

Middle East
+966 540 881 264
middleeast@iconics.co

Singapore
+65 6667 8295
singapore@iconics.com

UK
+44 1384 246 700
uk@iconics.com

For more, visit iconics.com

© 2020 ICONICS, Inc. All rights reserved. Specifications are subject to change without notice. AnalytiX and its respective modules are registered trademarks of ICONICS, Inc. GENESIS64, GENESIS32, Hyper Historian, BizViz, PortalWorX, MobileHMI and their respective modules, OPC-to-the-Core, and Visualize Your Enterprise are trademarks of ICONICS, Inc. Other product and company names mentioned herein may be trademarks of their respective owners.

Gold
Microsoft Partner
Six-time Partner of the Year Winner

VISUALIZE HISTORIZE MOBILIZE ANALYZE IoT CLOUD