Jonathan Andersson

joa@microsoft.com

Abstract

TechDays Sweden lab material about Operations Management Suite.

Modern management

from the cloud using Microsoft OMS

Table of Contents

[Prerequisites 3](#_Toc496558147)

[1 Log in to Azure 3](#_Toc496558148)

[2 Virtual Machines 3](#_Toc496558149)

[2.1 Create resource groups, virtual networks, Key Vault and two VMs 3](#_Toc496558150)

[2.2 Create a VM 4](#_Toc496558151)

[3 Log Analytics 4](#_Toc496558152)

[3.1 Get Started with Log Analytics 4](#_Toc496558153)

[3.2 Log Search in OMS Log Analytics Logs 5](#_Toc496558154)

[3.3 Custom Logs and Fields 5](#_Toc496558155)

[3.4 Custom View 5](#_Toc496558156)

[3.5 Extra assignment 6](#_Toc496558157)

[4 Automation 6](#_Toc496558158)

[4.1 Get started with Azure Automation 6](#_Toc496558159)

[4.2 Extra assignment 7](#_Toc496558160)

[4.3 Azure Automation Desired State Configuration 7](#_Toc496558161)

[4.3.3 Desired State Configuration Configurations 7](#_Toc496558162)

[4.4 Extra Resources 9](#_Toc496558163)

[5 Backup 9](#_Toc496558164)

[5.1 Backup an Azure VM 10](#_Toc496558165)

[6 Site Recovery 10](#_Toc496558166)

[6.1 Get Started with Azure Site Recovery (ASR) 10](#_Toc496558167)

[7 Security Center 11](#_Toc496558168)

[7.1 Get started 11](#_Toc496558169)

# Prerequisites

* Full rights in an Azure Subscription.
* PC that can access the Azure Portal.
* PC that can RDP and SSH to an Azure VM’s.

# Log in to Azure

Before we can start the labs, you need to make sure that you can log in to Azure:

Log in to Azure:

* Portal: Navigate to <http://portal.azure.com> and follow the login flow.
* PowerShell: <https://docs.microsoft.com/en-us/powershell/azure/authenticate-azureps?view=azurermps-4.3.1>
* Azure CLI: <https://docs.microsoft.com/en-us/cli/azure/get-started-with-azure-cli?view=azure-cli-latest>

# Virtual Machines

In the first lab, you will create a simple environment with one resource group for shared infrastructure and one resource group for the workload specific workloads. In the resource group for the shared infrastructure you will put virtual networks and things of that kind. In the resource group for workload specifics you will put VMs and resources that belongs to the VMs.

## Create resource groups, virtual networks and two VMs

Follow the steps below twice to create the resource groups. Name the first resource group *RG-Shared* and the second group *RG-Workloads*.

* + 1. Create one resource group named *RG-TechDays*.
* Portal: <https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-group-portal>
* PowerShell: <https://docs.microsoft.com/en-us/azure/azure-resource-manager/powershell-azure-resource-manager#create-a-resource-group>
* Azure CLI: <https://docs.microsoft.com/en-us/cli/azure/group?view=azure-cli-latest>
  + 1. Create a virtual network named *vnet-techdays* with a subnet named *subnet-techdays* in the resource group RG-TechDays.
* Portal: <https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-create-vnet-arm-pportal>
* PowerShell: <https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-create-vnet-arm-ps>
* Azure CLI: <https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-create-vnet-arm-cli>
* ARM Templates: <https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-create-vnet-arm-template-click>

## Create a VM

* + 1. Create an Azure VM in the resource groups *RG-TechDays*.
* Portal: <https://docs.microsoft.com/en-us/azure/virtual-machines/windows/quick-create-portal>.
* PowerShell: <https://docs.microsoft.com/en-us/azure/virtual-machines/windows/quick-create-powershell>
* Azure CLI: <https://docs.microsoft.com/en-us/azure/virtual-machines/windows/quick-create-cli>
* ARM: <https://azure.microsoft.com/en-us/resources/templates/101-vm-simple-windows/>

# Log Analytics

## Get Started with Log Analytics

In the following lab, you will get started with OMS Log Analytics. After completing the lab, you will have a Log Analytics Workspace created and configured. You will also have deployed your first OMS agent to an Azure VM and if you do not already have a VM to deploy to, you will also have a VM deployed.

Please do the following steps to get create and configure the Log Analytics workspace.

* + 1. Create and Configure a Log Analytics Workspace.
* <https://docs.microsoft.com/en-us/azure/log-analytics/log-analytics-quick-collect-azurevm#create-a-workspace>
  + 1. Add OMS Solutions.
* <https://docs.microsoft.com/en-us/azure/log-analytics/log-analytics-add-solutions>
  + 1. Install OMS agent on a VM.
* Windows agent: <https://docs.microsoft.com/en-us/azure/log-analytics/log-analytics-windows-agents>
* Linux agent: <https://docs.microsoft.com/en-us/azure/log-analytics/log-analytics-agent-linux>
* Azure VM: <https://docs.microsoft.com/en-us/azure/log-analytics/log-analytics-azure-vm-extension>
* Azure resources: <https://docs.microsoft.com/en-us/azure/log-analytics/log-analytics-azure-vm-extension>
* Operations Manager: <https://docs.microsoft.com/en-us/azure/log-analytics/log-analytics-om-agents>
  + 1. Add Windows events and Syslog logging.
* Windows Events: <https://docs.microsoft.com/en-us/azure/log-analytics/log-analytics-data-sources-windows-events>
* Syslog: <https://docs.microsoft.com/en-us/azure/log-analytics/log-analytics-data-sources-syslog>
  + 1. Add performance counters.
* Documentation: <https://docs.microsoft.com/en-us/azure/log-analytics/log-analytics-data-sources-performance-counters>

## Log Search in OMS Log Analytics Logs

When you have your OMS Log Analytics workspace created and it have started to import logs, you can start to search though them with Search in OMS Log Analytics.

* + 1. Try the different queries posted at the documentation
* <https://docs.microsoft.com/en-us/azure/log-analytics/log-analytics-tutorial-viewdata>
* <https://docs.microsoft.com/en-us/azure/log-analytics/log-analytics-log-search-new>
  + 1. Create Computer Group
* <https://docs.microsoft.com/en-us/azure/log-analytics/log-analytics-computer-groups>
  + 1. Act at results

To be able to do this lab you need to have an Automation Account created and a Runbook deployed.

* <https://docs.microsoft.com/en-us/azure/log-analytics/log-analytics-log-search-takeaction>
  + 1. Create an email alert

Try to create a query and send an email when for example the spooler service stops.

* <https://docs.microsoft.com/en-us/azure/log-analytics/log-analytics-alerts-creating#create-an-alert-rule>
  + 1. Create a new query from documentation
* <https://docs.loganalytics.io/index>

More documentation for complex queries

* <https://docs.loganalytics.io/docs/Learn/Tutorials/Getting-started-with-queries>
* <https://docs.loganalytics.io/docs/Examples/Log-Analytics-Examples>

## Custom Logs and Fields

Add a custom text log and create fields in Log Analytics.

* + 1. Add custom log
* <https://docs.microsoft.com/en-us/azure/log-analytics/log-analytics-data-sources-custom-logs>
  + 1. Create a custom field
* <https://docs.microsoft.com/en-us/azure/log-analytics/log-analytics-custom-fields>

## Custom View

Create a custom view for your search queries.

* + 1. Create a custom view
* <https://docs.microsoft.com/en-us/azure/log-analytics/log-analytics-view-designer>
  + 1. Add a custom view from a gallery
* Find a OMS view from the GitHub gallery and deploy it <https://github.com/Azure/azure-quickstart-templates>
* Search in the Azure Marketplace to see if you find a (free) OMS view to deploy.

## Extra assignment

Want to try more. Here are some extra labs for you.

Send data to Log Analytics with the HTTP Data Collector API

* <https://docs.microsoft.com/en-us/azure/log-analytics/log-analytics-data-collector-api>

Log Analytics REST API Reference

* <https://docs.microsoft.com/en-us/rest/api/loganalytics/>

Log Analytics PowerShell Module

* <https://docs.microsoft.com/en-us/powershell/module/azurerm.operationalinsights/?view=azurermps-4.4.0>

Manage Log Analytics using PowerShell

<https://docs.microsoft.com/en-us/azure/log-analytics/log-analytics-powershell-workspace-configuration>

# Automation

In this lab, you will familiarize yourself with Azure Automation. You will create your first Runbook and run it.

Azure Automation documentation: <https://docs.microsoft.com/en-us/azure/automation/>

## Get started with Azure Automation

* + 1. Create an Azure Automation Account
* <https://docs.microsoft.com/en-us/azure/automation/automation-offering-get-started#creating-an-automation-account>
  + 1. Create PowerShell runbook
* <https://docs.microsoft.com/en-us/azure/automation/automation-first-runbook-textual-powershell>
  + 1. Create PowerShell Workflow runbook and start it
* <https://docs.microsoft.com/en-us/azure/automation/automation-first-runbook-textual>
  + 1. Create graphical runbook and start it
* <https://docs.microsoft.com/en-us/azure/automation/automation-first-runbook-graphical>
  + 1. Runbook and module galleries for Azure Automation
* <https://docs.microsoft.com/en-us/azure/automation/automation-runbook-gallery>
  + 1. Testing a runbook in Azure Automation
* <https://docs.microsoft.com/en-us/azure/automation/automation-testing-runbook>
  + 1. Monitor a Runbook job
* <https://docs.microsoft.com/en-us/azure/automation/automation-runbook-execution>
  + 1. Install Automation Hybrid Runbook Worker
* <https://docs.microsoft.com/en-us/azure/automation/automation-hybrid-runbook-worker#installing-hybrid-runbook-worker>
  + 1. Start Runbook on Hybrid Runbook Worker
* <https://docs.microsoft.com/en-us/azure/automation/automation-hybrid-runbook-worker#starting-runbooks-on-hybrid-runbook-worker>

## Extra assignment

Want to try more. Here are some extra labs for you.

* + 1. Starting an Azure Automation runbook with a webhook
* <https://docs.microsoft.com/en-us/azure/automation/automation-webhooks>
  + 1. Runbook input parameters
* <https://docs.microsoft.com/en-us/azure/automation/automation-runbook-input-parameters>

## Azure Automation Desired State Configuration

In this lab, you will familiarize yourself with Azure Automation DSC. You will create your first DSC configuration, deploy and monitor.

* + 1. Create and deploy a DSC Configuration
* <https://docs.microsoft.com/en-us/azure/automation/automation-dsc-getting-started>
  + 1. Forward Azure Automation DSC reporting data to OMS Log Analytics
* <https://docs.microsoft.com/en-us/azure/automation/automation-dsc-diagnostics>

### Desired State Configuration Configurations

#### Windows DSC IIS Configuration

Configuration WinIISFeature

{

Import-DscResource –ModuleName ’PSDesiredStateConfiguration’

Node localhost

{

#Install IIS

WindowsFeature IIS

{

Ensure = "Present"

Name = "Web-Server"

}

}

}

#### Red Hat DSC Httpd Configuration

Configuration LinuxWebYum

{

Import-DSCResource -Module nx

Node "httpd"

{

nxPackage httpdInstall

{

Name = "httpd"

Ensure = "Present"

PackageManager = "Yum"

}

nxService httpdService

{

Name = "httpd"

Controller = "systemd"

Enabled = $true

State = "Running"

}

nxFile httpdFile

{

Ensure = "Present"

Type = "File"

DestinationPath = "/var/www/html/index.html"

Contents = '<!DOCTYPE html>

<html>

<head>

<title>My DSC Linux Apache Test Page</title>

</head>

<body bgcolor="#00c87c">

<h3 style="color:blue">This Httpd server and webpage is installed and configured by DSC on Linux</h3>

</body>

</html>'

}

}

}

#### Ubuntu DSC Httpd Configuration

Configuration LinuxWebApt

{

Import-DSCResource -Module nx

Node "apache2"

{

nxPackage apache2Install

{

Name = "apache2"

Ensure = "Present"

PackageManager = "Apt"

}

nxService apache2Service

{

Name = "apache2"

Controller = "init"

Enabled = $true

State = "Running"

}

nxFile apache2File

{

Ensure = "Present"

Type = "File"

DestinationPath = "/var/www/index.html"

Contents = '<!DOCTYPE html>

<html>

<head>

<title>My DSC Linux Apache Test Page</title>

</head>

<body bgcolor="#00c87c">

<h3 style="color:blue">This Apache server and webpage is installed and configured by DSC on Linux</h3>

</body>

</html>'

}

}

}

## Extra Resources

Get started with Desired State Configuration (DSC) for Linux

* <https://docs.microsoft.com/en-us/powershell/dsc/lnxgettingstarted>
* <https://docs.microsoft.com/en-us/powershell/dsc/lnxpackageresource>
* <https://github.com/Microsoft/PowerShell-DSC-for-Linux>

# Backup

Azure Backup is the Azure-based service you can use to back up (or protect) and restore your data in the Microsoft cloud. Azure Backup replaces your existing on-premises or off-site backup solution with a cloud-based solution that is reliable, secure, and cost-competitive. Azure Backup offers multiple components that you download and deploy on the appropriate computer, server, or in the cloud. The component, or agent, that you deploy depends on what you want to protect. All Azure Backup components (no matter whether you're protecting data on-premises or in the cloud) can be used to back up data to a Recovery Services vault in Azure.

<https://docs.microsoft.com/en-us/azure/backup/backup-introduction-to-azure-backup>

## Backup an Azure VM

* + 1. Create a recovery services vault
* <https://docs.microsoft.com/en-us/azure/backup/backup-azure-arm-vms-prepare#create-a-recovery-services-vault-for-a-vm>
  + 1. Select a backup goal, set policy and define items to protect
* <https://docs.microsoft.com/en-us/azure/backup/backup-azure-arm-vms-prepare#select-a-backup-goal-set-policy-and-define-items-to-protect>
  + 1. Backup the Azure VM
* <https://docs.microsoft.com/en-us/azure/backup/backup-azure-arm-vms>
  + 1. Restore Azure VM
* <https://docs.microsoft.com/en-us/azure/backup/backup-azure-arm-restore-vms>
  + 1. Restore files in Azure VM
* <https://docs.microsoft.com/en-us/azure/backup/backup-azure-restore-files-from-vm>

# Site Recovery

In the following lab, you will setup ASR. If you have the possibility to do it in your own environment please use step 1. If you don’t, please use step 2 and set up ASR between two Azure datacenters. After setup is done, please go to step 3. If you want to read what ASR is read this overview <https://docs.microsoft.com/en-us/azure/site-recovery/site-recovery-overview>.

ASR documentation: <https://docs.microsoft.com/en-us/azure/site-recovery/>

## Get Started with Azure Site Recovery (ASR)

* + 1. Setup ASR. Please go to the documentation for your environment.
* VmWare to Azure: <https://docs.microsoft.com/en-us/azure/site-recovery/vmware-walkthrough-overview>
  + Quick start, go to step 7 in the documentation.
* Hyper-V to Azure: <https://docs.microsoft.com/en-us/azure/site-recovery/hyper-v-site-walkthrough-overview>
* Hyper-V virtual machines in VMM clouds to Azure: <https://docs.microsoft.com/en-us/azure/site-recovery/site-recovery-vmm-to-azure>
* Physical servers to Azure: <https://docs.microsoft.com/en-us/azure/site-recovery/physical-walkthrough-overview>
  + 1. Azure to Azure
* <https://docs.microsoft.com/en-us/azure/site-recovery/site-recovery-azure-to-azure>
  + 1. Create recovery plans
* <https://docs.microsoft.com/en-us/azure/site-recovery/site-recovery-create-recovery-plans>
  + 1. Run a test failover for a plan
* <https://docs.microsoft.com/en-us/azure/site-recovery/site-recovery-test-failover-to-azure>
  + 1. Migrate VM’s to Azure
* <https://docs.microsoft.com/en-us/azure/site-recovery/site-recovery-migrate-to-azure>

For more information regarding workloads please see the following: <https://docs.microsoft.com/en-us/azure/site-recovery/site-recovery-workload>

# Security Center

Security Center helps you prevent, detect, and respond to threats with increased visibility into and control over the security of your Azure resources. It provides integrated security monitoring and policy management across your Azure subscriptions, helps detect threats that might otherwise go unnoticed, and works with a broad ecosystem of security solutions.

## Get started

In this lab, you will setup and configure Security Center.

* + 1. Enable Security Center
* <https://docs.microsoft.com/en-us/azure/security-center/security-center-get-started#access-security-center>
  + 1. Set security policies in Azure Security Center
* <https://docs.microsoft.com/en-us/azure/security-center/security-center-policies>
  + 1. Managing security recommendations
* <https://docs.microsoft.com/en-us/azure/security-center/security-center-recommendations>
  + 1. Manage virtual machine access using just in time
* <https://docs.microsoft.com/en-us/azure/security-center/security-center-just-in-time>