**Azure Standard Load Balancer with an IaaS Web Application**



Author(s) / Document Version Control Information

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Author** | **Description** | **Version** |
| 5/23/2019 | Roger A. Dahlman | Initial Revision | 1.0 |
| 6/17/2019 | Daniel A. Bachrach | Insertion of Appendix A | 1.1 |
| 7/19/2019 | Roger A. Dahlman  Venkateshwarlu P. Goud | Added implementation on controls | 1.2 |

**TABLE OF CONTENTS**

[1 Recipe Targets 2](#_Toc11664231)

[2 Recipe Scenario 2](#_Toc11664232)

[3 Recipe Architecture 2](#_Toc11664233)

[4 Pertinent Cloud Component Details 3](#_Toc11664234)

[5 Constraints and Limitations 5](#_Toc11664235)

[6 APPENDIX A – Control Reference 6](#_Toc11664236)

# Recipe Targets

* **Cloud Platform:** Azure
* **Application Type**: Internal application with sensitive data. Lift and Shift applications in general.
* **Compliance Target**: SOC2 Type 2, ISO 2700x
* **Data Classifications**: PII, PHI, Customer Confidential, and Firm Confidential
* **Primary Cloud Services:** Azure Standard Load Balancer, IaaS, Deloitte HUB
* **Geographies**: All

# Recipe Scenario

This recipe targets Web applications hosted in a cluster of Azure IaaS VMs leveraging any OS and web server such as IIS. The scenario targets internal Deloitte applications that need to be compliant with PM40 and other Deloitte Cyber Security standards. The recipe was used specifically for a globally hosted US application that utilizes OneCloud provisioned VMs and the OneCloud Deloitte HUB for internet connectivity. The scenario was the result of a lift and shift migration of a Deloitte on premises application. Beyond Windows AD services provided by the Deloitte HUB no connectivity to the Deloitte on premises services was required. The recipe does not target or cover a database technology nor a disaster recovery scenario.

# Recipe Architecture

The diagram below illustrates the conceptual Azure architecture of the recipe.



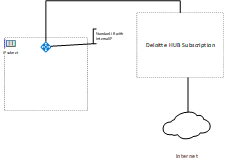
As one can see from the diagram all internet traffic ingress and egress from the Azure subscription goes through a Deloitte HUB subscription to mitigate cyber security threats (Team n.d.). Traffic ingress from the internet flows from the Deloitte HUB subscription to the Deloitte target subscription by leveraging VNet peering to a Vnet with a single subnet within the target Azure subscription (the one hosting the application).  
  
The subnet mentioned above contains all of the application’s infrastructure consisting of an Azure Standard Internal Load Balancer, two IaaS VMs hosting Windows Server and IIS in an Azure Availability Set (any firm approved OS and web server could be used). It should be noted that more than 2 VMs can be used in this recipe.

# Pertinent Cloud Component Details

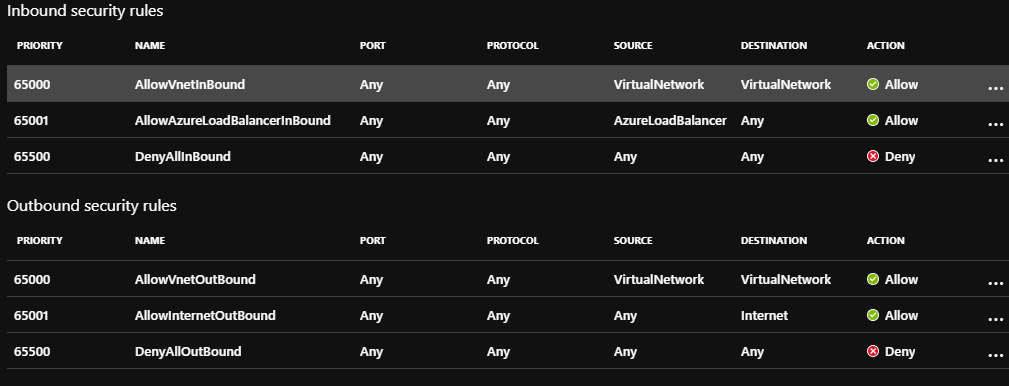
**Deloitte HUB**

The Deloitte HUB can be thought of as a Deloitte SaaS service that provides a web application firewall (WAF) and enforces Cyber Security controls on internet traffic. This allows Cyber Security and other entities within Deloitte to ensure the application is protected from common security threats and that malicious traffic is tracked.

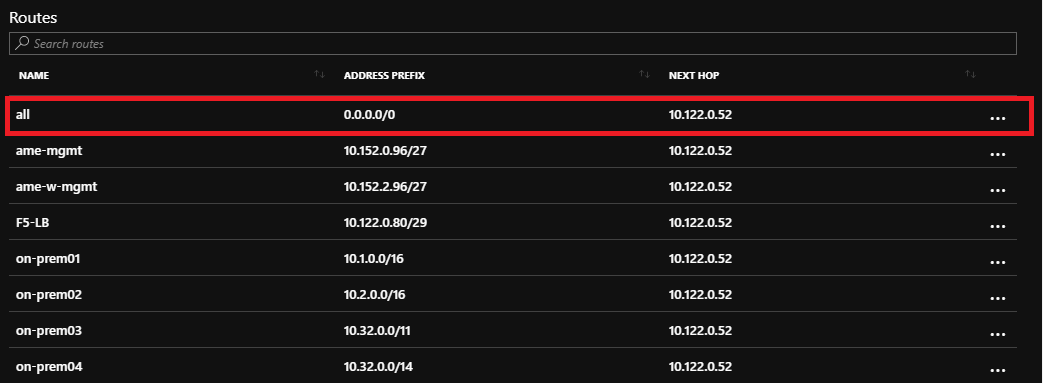
The HUB is used to communicate from the internet to the load balancer. To achieve this goal an external IP was requested from the networking team. This IP was then configured by the networking team to route all traffic from port 443 to the IP used for the Azure Standard Internal Load Balancer. As you can see from the diagram below traffic from the Deloitte HUB simply enters the load balancer as if it came from an Azure internet IP associated with an Azure Standard External Load Balancer.

  
**Azure Standard Internal Load Balancer**   
The Azure Standard Internal Load Balancer was assigned an IP address on the same subnet as the Azure IaaS VMs. The VMs where assigned to the load balancer’s backend pool so that traffic entering the load balancer could be distributed between them using load balancing rules. One “load balancing rules” where created, one for port 443. The load balancing rule required a health probe to determine if the VMs in the backend pools are running. One health probe was created targeting the TCP protocol and was assigned to probe port 443 and assigned to the load balancing rule with the same target port, 443. It is important to note that TCP was targeted for the probe. Initially HTTP was targeted but this caused the cluster to go down unexpectedly. This was because health probes do not support HTTP Host Headers so it could not receive a response from the VMs since all sites hosted used Host Headers. A work around could have been to setup a default site using a port other than 443 for HTTP but it was determined that it was cleaner and required less server maintenance to just probe TCP.

The Azure Internal Standard Load Balancer also required special network configuration to ensure the load balancer could talk to the VMs and the VMs to contact external web services on the internet. By default, the Standard Load Balancer does not allow communications between the load balancer and VMs so a network security group was created to allow traffic to and from the load balancer and to the Deloitte HUB subscription as illustrated below.



It was additionally necessary to modify the route table to route all unhandled traffic to the hub subscription for outbound internet connectivity. This ensures all traffic is scanned by the HUB. A sample configuration is illustrated below.



The route highlighted in red sends all unhandled traffic to the Deloitte HUB. Specifically, in this example it sends traffic to a F5 virtual appliance in the HUB at IP address 10.122.0.52. Be careful not to make assumption about the HUBs internals because the F5s or any other components could be replaced in the future. This implementation is very specific to Deloitte’s networking strategy.

**Availability Set**   
An Availability Set was used in this recipe but with increased cost it could be replaced with an Availability Zone if there is a desire to increase resiliency.

**Vnet/Subnet** 

As mentioned previously the VNET was peered with the HUB subscription to allow for internet traffic to flow to the load balancer and out of the VMs. The route table changes in the Azure Standard Internal Load Balancer section above were required.

**IaaS VM**

The IaaS VM in this scenario functions as a web server connecting to a backend datastore on the same subnet. HTTP Host Headers are used to host multiple sites. Port 443 is utilized for internet traffic.

Important: All VMs in the recipe were provisioned using OneCloud Cloud Script which ensures Puppet is installed on the VMs. This allows the VMs to be patched to Deloitte standards and ensure appropriate Cyber Security services are installed. You can learn more about OneCloud at <http://onecloud.deloitte.com>.

# Constraints and Limitations

This recipe is recommended for quick lift and shift migrations of on premises applications that do not have greater than a tier 3 BCP requirement. An Azure Internal Standard Load Balancer was chosen specifically because it is a lightweight level three load balancer that easily mimics on premises concepts.

While this recipe as it stands does not provide a high degree of business continuity adding Azure Traffic manager and Azure site recovery will enhance it to meet most business continuity needs. An updated recipe with be added soon to cover this scenario. Additionally, if designing Cloud Native applications, you should consider an all PaaS solution or if you do require IaaS web servers an Azure Application Gateway would provide more advanced capabilities but comes at a higher cost and requires its own subnet. The new Azure Front Door service could also be considered for very advanced scenarios that might not require a HUB subscription. At present we do not have applications that use Front Door but that may change in time.

# APPENDIX A – Control Reference

|  |  |  |  |
| --- | --- | --- | --- |
| **Control requirement** | **Control #** | **Control Description** | **Implementation Requirements** |
| **Cyber Risk Management, Metrics & Reporting** | **IT- 51** | IPS events are logged into Security Incident and Event Management (SIEM) and monitored by Security Operations Center (SOC). | • Log Intrusion Prevention System (IPS) events into SIEM (Security Incident and Event Management) and integrate for monitoring with the Security Operations Center (SOC) • Monitor IPS logs continuously for alerts and suspicious network activity |
| **Implementation** | The Recipe’s architecture ensures that all HTTP traffic from the web frontend flows through an **internal** Deloitte network IP on port 443 exposed by an internal load balancer. To be more specific the Recipe’s internal load balancer is only configured to allow inbound HTTP egress from the internal Deloitte network. Internal and external users can only access the internal HTTP endpoint if traffic is routed to the internal load balancer through additional network configurations. As an example, the network team could allow external user HTTP requests to be routed to the load balancer’s internal IP through a Deloitte HUB subscription[[1]](#footnote-1) with VNet peering. This network configuration addresses the specified IPS requirement given it inherits compliance from mechanisms configurated by the networking. The recipe does not provide any mechanism to configure a means to expose traffic directly on the internet or internal Deloitte network other than the previously mentioned endpoint on the internal load balancer. | |
| **Data Privacy** | **DS-10** | Sensitive information must not be stored in log files | • Ensure any sensitive and critical information, which has been classified as confidential information (CI) based on the data classification guidelines, is not stored in application and platform related logs |
| **Implementation** | The Azure VMs and Load Balancer deployed by the Recipe by default do not have contain sensitive information to expose. Application deployed on the VMs will be responsible for implementing this controls at the application level. | |
| **Encryption** | **DS-14** | Encryption in transit is used to transfer data between end users and the Cloud environment using a protocol that is authorized in accordance with Deloitte Encryption & Key Management Standards | • Use HTTPS for in-transit encryption for web access, Virtual Private Network (VPN), and remote consoles • Configure the following Transport Layer Security (TLS) minimum requirements as per Deloitte standards:  o Version - TLS v1.1 and higher  o Public key size - RSA 2048 bit  o Certificate Signing - SHA2 • Configure F5 load balancers to redirect traffic to HTTPS (if it comes in as HTTP)  ***Note:*** *The option to disable TLS 1.0 completely is not available yet.* |
| **Implementation** | The Recipe’s architecture ensures that all HTTP traffic from the web frontend flows through an **internal** Deloitte network IP on port 443 exposed by an internal load balancer. To be more specific the Recipe’s internal load balancer is only configured to allow inbound HTTP egress from the internal Deloitte network. Internal and external users can only access the internal HTTP endpoint if traffic is routed to the internal load balancer through additional network configurations. As an example, the network team could allow external user HTTP requests to be routed to the load balancer’s internal IP through a Deloitte HUB subscription[[2]](#footnote-2) with VNet peering. This network configuration addresses the specified encryption in transit requirement given it inherits compliance from mechanisms configurated by the networking team and further promotes encryption by only allowing the SSL port 443 to be opened. The recipe does not provide any mechanism to configure a means to expose traffic directly on the internet or internal Deloitte network other than the previously mentioned endpoint on the internal load balancer. | |
| **DS-18** | All traffic between end users and Cloud hosted applications must be encrypted when routed over the Internet | • Use HTTPS for in-transit encryption for web access, VPN, and remote consoles • Configure the following Transport Layer Security (TLS) minimum requirements as per Deloitte standards document:  o Version - TLS v1.1 and higher  o Public key size - RSA 2048 bit  o Certificate Signing - SHA2 • Configure F5 load balancers to redirect traffic to HTTPS (if it comes in as HTTP)  ***Note:*** *The option to disable TLS 1.0 completely is not available yet.* |
| **Implementation** | The Recipe’s architecture ensures that all HTTP traffic from the web frontend flows through an **internal** Deloitte network IP on port 443 exposed by an internal load balancer. To be more specific the Recipe’s internal load balancer is only configured to allow inbound HTTP egress from the internal Deloitte network. Internal and external users can only access the internal HTTP endpoint if traffic is routed to the internal load balancer through additional network configurations. As an example, the network team could allow external user HTTP requests to be routed to the load balancer’s internal IP through a Deloitte HUB subscription[[3]](#footnote-3) with VNet peering. This network configuration addresses the specified encryption requirement given it inherits compliance from mechanisms configurated by the networking team and further promotes encryption by only allowing the SSL port 443 to be opened. The recipe does not provide any mechanism to configure a means to expose traffic directly on the internet or internal Deloitte network other than the previously mentioned endpoint on the internal load balancer. | |
| **Identity Lifecycle Management** | **IT-34** | Access provisioning procedures are in place to restrict access on a need-to-have basis for internal users; privileged access requests require approval of the user's manager as well as the manager over the privileged role | • Ensure that for internal users, an access request form is completed on the security website; logged by the resource manager with business need along with the specific component that the resource needs access for; and sent for approval from the project manager • Provision all privileged access on a need-to-have basis per the Deloitte access provisioning and deprovisioning standards and procedures |
| **Implementation** | Given that the OneCOP API[[4]](#footnote-4)ensures compliant Deloitte VM Images are deployed only Active Directory security groups will be given access to VMs at any level. The PAM tool must to used to request additional access for any user that is added to an Active Directory security group. Administrative access to Azure infrastructure in the Recipe is controlled at the Azure control plane. Access to the control plane is managed by member firm standards that require a SPN be acquired to allow the Recipe to be deployed. Once deployed infrastructure components of the Recipe inherit control plane access Active Directory groups defined in their containing Azure Resource Group. | |
| **Network Security** | **IT-38** | Intrusion Prevention Systems (IPS) are in place on the network and are updated for the latest rule set on a regular basis (at least weekly). | • Deploy IPS devices to monitor all Azure subscriptions – including subscriptions associated with the audit applications as well as hub subscriptions hosting cloud network components • Deploy IPS sensors at the gateways in inline mode (detect / prevent) • Employ a centralized tool / console to manage IPS sensors and rule-sets • Review and update IPS rule-sets on a weekly basis |
| **Implementation** | The Recipe’s architecture ensures that all HTTP traffic from the web frontend flows through an **internal** Deloitte network IP on port 443 exposed by an internal load balancer. To be more specific the Recipe’s internal load balancer is only configured to allow inbound HTTP egress from the internal Deloitte network. Internal and external users can only access the internal HTTP endpoint if traffic is routed to the internal load balancer through additional network configurations. As an example, the network team could allow external user HTTP requests to be routed to the load balancer’s internal IP through a Deloitte HUB subscription[[5]](#footnote-5) with VNet peering. This network configuration addresses the specified IDS/IPS requirement given it inherits compliance from mechanisms configurated by the networking. The recipe does not provide any mechanism to configure a means to expose traffic directly on the internet or internal Deloitte network other than the previously mentioned endpoint on the internal load balancer. | |
| **IT-39** | Firewalls are in place to prevent unauthorized access to the corporate network. New firewall rules or changes to existing firewall rules are approved prior to being implemented | • Deploy and configure F5 firewalls to prevent unauthorized access to the corporate network • Ensure any new firewall rules or changes made to the existing firewall rules are tracked, are assigned to the appropriate personnel for approval, and a ticket is associated with every change request, per the Firewall Change Management process |
| **Implementation** | The Recipe’s architecture ensures that all HTTP traffic from the web frontend flows through an **internal** Deloitte network IP on port 443 exposed by an internal load balancer. To be more specific the Recipe’s internal load balancer is only configured to allow inbound HTTP egress from the internal Deloitte network. Internal and external users can only access the internal HTTP endpoint if traffic is routed to the internal load balancer through additional network configurations. As an example, the network team could allow external user HTTP requests to be routed to the load balancer’s internal IP through a Deloitte HUB subscription[[6]](#footnote-6) with VNet peering. This network configuration addresses the specified firewall requirement given it inherits compliance from mechanisms configurated by the networking team. The recipe does not provide any mechanism to configure a means to expose traffic directly on the internet or internal Deloitte network other than the previously mentioned endpoint on the internal load balancer. | |
| **Privileged User Access Control** | **IT-36** | Privileged access to sensitive resources is restricted to defined user roles, and access to these roles must be approved by the respective data owner. This access is reviewed by the respective data owner on a periodic basis | • Provision all privileged access, considering the following principles, per the Deloitte access provisioning standards and procedures:  o Least-privilege - Everything is generally forbidden unless expressly permitted  o Need-to-know  o Segregation of duties and roles, as defined by Application / System and / or Business Owner (e.g., access request, access authorization, access administration, audit) • For each privileged access request, ensure that the Elevated Access Form is completed with the type of access, description and approver details • Leverage Azure Role-Based Access Control (RBAC) within the Azure subscriptions to enable fine-grained access management by allowing access for job-only related activities • Functions that make calls to protected resources (e.g., Azure Key Vault) must adhere to Deloitte access and provisioning standards • Creation of a function code must be restricted and should leverage RBAC |
| **Implementation** | Given that the OneCOP API[[7]](#footnote-7)ensures compliant Deloitte VM Images are deployed and only Active Directory security groups will be given access to VMs at any level. The PAM tool must to used to request additional access for any user that is added to an Active Directory security group. Administrative access to Azure infrastructure in the Recipe is controlled at the Azure control plane. Access to the control plane is managed by member firm standards that require a SPN be acquired to allow the Recipe to be deployed. Once deployed infrastructure components of the Recipe inherit control plane access Active Directory groups defined in their containing Azure Resource Group. | |
| **Secure Software Development Lifecycle** | **DS-24** | Cloud hosted applications must have built in redundancy to ensure continuous operations when availability is interrupted in their primary hosting location | • Leverage Microsoft Azure’s built-in redundancy for SaaS services |
| **Implementation** | All applications in Deloitte must have a BCP plan and to ensure compliance. | |
| **IT-58** | Networking capacity is monitored on an ongoing basis | • Monitor network capacity and utilization on an ongoing basis using a centralized network and capacity logging and monitoring tool • Configure the network and capacity logging and monitoring tool to provide overview of the following on the dashboard:  o All nodes;  o Overall hardware health;  o Top 10 interfaces by utilization; and  o Top 10 interfaces by performance • For each node, configure the network and capacity logging and monitoring tool to document and display the following:  o Node status;  o IP address;   o Machine type;   o Average response time;   o Packet loss;   o CPU load;  o Memory used;  o Overall hardware status; and   o Net flow version • Configure generation of automated alerts, and creation of ticket when a node is down • Conduct monthly meetings to review capacity monitoring currently in-place and to resolve any capacity management efforts for the incoming month |
| **Implementation** | Given that the OneCOP API[[8]](#footnote-8)ensures compliant Deloitte VM Images are deployed and only Active Directory security groups will be given access to VMs at any level. The PAM tool must to used to request additional access for any user that is added to an Active Directory security group. Administrative access to Azure infrastructure in the Recipe is controlled at the Azure control plane. Access to the control plane is managed by member firm standards that require a SPN be acquired to allow the Recipe to be deployed. Once deployed infrastructure components of the Recipe inherit control plane access Active Directory groups defined in their containing Azure Resource Group. These tools include Deloitte standard VM monitoring tools and VM configuration. | |
| **Security Platform Administration & Operations** | **CI-05** | Cloud-hosted applications have a production environment that is logically segregated from its lesser environments | • Logically segregate production and non-production environments by maintaining distinct Virtual Network • Perform Quality Assurance (QA) testing, load testing and other related activities on non-production subscriptions. Ensure no cross-over of data happens between the environments |
| **Implementation** | Recipe is installed within a given environment such as PROD or QA. Recipe will need to be deployed in each application environment. | |
| **System Security** | **CI-12** | Cloud-hosted applications are deployed using reviewed and approved infrastructure templates that abide by minimum baseline security configurations | • Use approved infrastructure templates for deployment of Cloud-hosted applications |
| **Implementation** | Given that the OneCOP API[[9]](#footnote-9)ensures compliant Deloitte VM Images are deployed and only Active Directory security groups will be given access to VMs at any level. The PAM tool must to used to request additional access for any user that is added to an Active Directory security group. Administrative access to Azure infrastructure in the Recipe is controlled at the Azure control plane. Access to the control plane is managed by member firm standards that require a SPN be acquired to allow the Recipe to be deployed. Once deployed infrastructure components of the Recipe inherit control plane access Active Directory groups defined in their containing Azure Resource Group. | |
| **IT-24** | Secure systems configuration standards are defined for each server and workstation operating system used within the system | • Use approved infrastructure templates for deployment of Cloud-hosted applications |
| **Implementation** | Given that the OneCOP API[[10]](#footnote-10)ensures compliant Deloitte VM Images are deployed. | |
| **User Access Control** | **CI-04b** | All communication between a user and an Azure hosted global solution must be first authenticated using one of the following solutions: • Internal Deloitte users: Azure Active Directory or ADFS  • External users: Azure B2B or DPASS | • Integrate with Azure AD for imposing authentication and authorization controls |
| **Implementation** | The Recipe does not control the authentication method used by an application installed on the Web Server VMs. That said its architecture allows for the use of Azure Active Directory, ADFS, DPASS and Azure B2B. The authentication method will have to validated with the application level controls. | |

1. A Deloitte hub subscription is a pattern followed the networking team to securely route traffic both from the internet and on-premises network following networking and Cyber Security best practices. IDS/IPS and other attack mitigation techniques are followed per Cyber Security requirements. [↑](#footnote-ref-1)
2. A Deloitte hub subscription is a pattern followed the networking team to securely route traffic both from the internet and on-premises network following networking and Cyber Security best practices. IDS/IPS and other attack mitigation techniques are followed per Cyber Security requirements. [↑](#footnote-ref-2)
3. A Deloitte hub subscription is a pattern followed the networking team to securely route traffic both from the internet and on-premises network following networking and Cyber Security best practices. IDS/IPS and other attack mitigation techniques are followed per Cyber Security requirements. [↑](#footnote-ref-3)
4. The OneCOP API is a Deloitte OneCloud VM management API that ensures all VMs it creates use Deloitte standard VM images and follow member firm standards. This API installs Puppet on all VMs to ensure that Cyber Security and other tools required for security and compliances are installed on VMs. [↑](#footnote-ref-4)
5. A Deloitte hub subscription is a pattern followed the networking team to securely route traffic both from the internet and on-premises network following networking and Cyber Security best practices. IDS/IPS and other attack mitigation techniques are followed per Cyber Security requirements. [↑](#footnote-ref-5)
6. A Deloitte hub subscription is a pattern followed the networking team to securely route traffic both from the internet and on-premises network following networking and Cyber Security best practices. IDS/IPS and other attack mitigation techniques are followed per Cyber Security requirements. [↑](#footnote-ref-6)
7. The OneCOP API is a Deloitte OneCloud VM management API that ensures all VMs it creates use Deloitte standard VM images and follow member firm standards. This API installs Puppet on all VMs to ensure that Cyber Security and other tools required for security and compliances are installed on VMs. [↑](#footnote-ref-7)
8. The OneCOP API is a Deloitte OneCloud VM management API that ensures all VMs it creates use Deloitte standard VM images and follow member firm standards. This API installs Puppet on all VMs to ensure that Cyber Security and other tools required for security and compliances are installed on VMs. [↑](#footnote-ref-8)
9. The OneCOP API is a Deloitte OneCloud VM management API that ensures all VMs it creates use Deloitte standard VM images and follow member firm standards. This API installs Puppet on all VMs to ensure that Cyber Security and other tools required for security and compliances are installed on VMs. [↑](#footnote-ref-9)
10. The OneCOP API is a Deloitte OneCloud VM management API that ensures all VMs it creates use Deloitte standard VM images and follow member firm standards. This API installs Puppet on all VMs to ensure that Cyber Security and other tools required for security and compliances are installed on VMs. [↑](#footnote-ref-10)