MANAGED MICROSOFT AZURE SERVICES

Service Level Description (SLD)

December 6, 2017
# Table of Contents

1. **PURPOSE** ......................................................................................................................... 4

2. **INTRODUCTION** .............................................................................................................. 4

3. **SUPPORTED AZURE SERVICES** ....................................................................................... 4

4. **MICROSOFT AZURE ARCHITECTURE** .............................................................................. 5
   4.1 **VIRTUAL MACHINES** .................................................................................................... 5
   4.2 **AVAILABILITY SETS** .................................................................................................... 6
   4.3 **VM STORAGE** ............................................................................................................... 6
   4.4 **STANDALONE STORAGE** ............................................................................................ 7
   4.5 **NETWORKING** ............................................................................................................. 8
       4.5.1 Virtual Network Benefits ............................................................................................ 8
       4.5.2 Subnets ....................................................................................................................... 9
       4.5.3 IP addresses .............................................................................................................. 9
       4.5.4 Azure load balancers ................................................................................................. 9
       4.5.5 Azure Traffic Manager ............................................................................................ 10
       4.5.6 Network Security Group (NSG) ................................................................................ 11
       4.5.7 Routing ..................................................................................................................... 11
       4.5.8 VPN Gateways .......................................................................................................... 12
       4.5.9 Express Route ........................................................................................................... 12
   4.6 **LICENSE MODELS** ....................................................................................................... 12

5. **SERVICE DESCRIPTION** ................................................................................................... 13
   5.1 **SERVICE AVAILABILITY** ............................................................................................ 13
   5.2 **DESIGN DOCUMENT CREATION** ............................................................................. 13
   5.3 **PROVISIONING OF MICROSOFT AZURE ACCOUNT** ............................................... 14
   5.4 **NETWORK IMPLEMENTATION** .................................................................................. 14
   5.5 **DNS IMPLEMENTATION** ............................................................................................. 14
   5.6 **AVAILABILITY GROUP/VIRTUAL MACHINE IMPLEMENTATION** ............................ 14
   5.7 **BLOB STORAGE IMPLEMENTATION** ........................................................................ 14
   5.8 **LOAD BALANCER IMPLEMENTATION** ...................................................................... 15
   5.9 **BACKUP IMPLEMENTATION** .................................................................................... 15
   5.10 **AZURE IMPORT/EXPORT SERVICE** ....................................................................... 15
   5.11 **IMPLEMENTATION OF THE NAVISITE MONITORING PLATFORM** ...................... 15

6. **MONTHLY SERVICE DESCRIPTION** ................................................................................ 16
   6.1 **DESIGN UPDATES** ..................................................................................................... 16
   6.2 **OS MONITORING SERVICES** ..................................................................................... 16
       6.2.1 **NAVISITE RESPONSIBILITIES / ACTIVITIES** ...................................................... 16
   6.3 **NETWORK MANAGEMENT** ....................................................................................... 16
   6.4 **OS MANAGEMENT SERVICE** .................................................................................... 17
       6.4.1 **ONGOING OPERATIONAL MANAGEMENT** ........................................................ 17
       6.4.2 **FAULT MANAGEMENT** ....................................................................................... 17
       6.4.3 **WINDOWS PATCH MANAGEMENT** .................................................................... 17
6.4.3.1 Emergency patch procedures for security related issues .................................................. 18
6.4.3.2 Non-Emergency patch procedures for performance related issues .................................. 18
6.4.4 LINUX PATCH MANAGEMENT .................................................................................. 19
6.4.5 CUSTOMER RESPONSIBILITIES: .............................................................................. 19
6.5 BLOB STORAGE MANAGEMENT ...................................................................................... 19
6.6 LOAD BALANCER MANAGEMENT ................................................................................... 19

7. RACI’S ................................................................................................................................. 21
7.1 WINDOWS SYSTEMS MANAGEMENT .............................................................................. 21
7.2 LINUX SYSTEMS MANAGEMENT ..................................................................................... 22
1. PURPOSE
This Service Level Description details the services provided by Navisite as well as client requirements for the Managed Azure product line. This document is not a legal or binding agreement; instead, it is intended to be an operational description of a Navisite Service.

Confidential Information Notice
The information contained herein is hereby marked NAVISITE CONFIDENTIAL, is intended only for the use of the individual or individuals to which it is addressed, and shall not be disclosed or made available to any other party except with the prior written consent of NAVISITE. This proprietary data may not be duplicated, distributed, or disclosed in whole or part.

2. INTRODUCTION
This service description details Navisite’s Managed Azure services (Managed Azure). Managed Azure provides companies with a fully managed cloud environment where the network and operating systems are tailored and managed to meet the requirements of each Customer’s application and/or infrastructure environment. This service allows for the union of the highly scalable and stable Microsoft Azure cloud with Navisite’s comprehensive management services. The Managed Azure service provides comprehensive 24x7 managed hosting services including:

- VM provisioning and management
- VM backups
- Networking management including connectivity, load balancers, and firewalls

3. SUPPORTED AZURE SERVICES
Microsoft provides many different services under their Azure umbrella, some of which can be managed by Navisite in support of a fully managed solution. Specifically the services that are supported are:

<table>
<thead>
<tr>
<th>Microsoft Azure Service</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual Machines</td>
<td>Provision Windows and Linux Virtual Machines and applications in minutes</td>
</tr>
<tr>
<td>Storage</td>
<td>Durable, highly available and massively scalable cloud storage</td>
</tr>
<tr>
<td>Backup</td>
<td>Simple and reliable server backup via Navisite’s Unified Backup platform</td>
</tr>
<tr>
<td>Virtual Network</td>
<td>Provision private networks, optionally connect to on-premises datacenters</td>
</tr>
<tr>
<td>Load Balancer</td>
<td>Deliver high availability and network performance to your applications</td>
</tr>
<tr>
<td>VPN Gateway</td>
<td>Establish secure, cross-premises connectivity</td>
</tr>
</tbody>
</table>
4. MICROSOFT AZURE ARCHITECTURE

Microsoft Azure Services are comprised of many, many components which are configured and managed by Navisite in an optimal manner to meet customer requirements. While these components have countless permutations for combination, Navisite has developed templates to ensure that all services can be delivered in a stable and secure manner while still allowing a sufficient amount of customization for each individual customer. The major components of a Navisite managed Azure environment are described below.

4.1 Virtual Machines

Azure Virtual Machines is one of several types of on-demand, scalable computing resources that Azure offers. An Azure virtual machine gives you the flexibility of virtualization without having to buy and maintain the physical hardware that runs the virtual machine. However, you still need to maintain the virtual machine -- configuring, patching, and maintaining the operating system and any other software that runs on the virtual machine.

Azure Virtual Machines lets you create and use virtual machines in the cloud. Providing what's known as Infrastructure as a Service (IaaS), virtual machine technology can be used in variety of ways. Like other virtual machines, a VM in Azure has an operating system, storage and networking capabilities and can run a wide variety of applications. Navisite provides pre-defined templates with all required management and monitoring components pre-installed.

Virtual machines use virtual hard disks (VHDS) to store their operating system (OS) and data. VHDS are also used for the images you can choose from to install an OS. The following figure shows this, as well as two of the tools Navisite may use for creating and managing your VMs.
Along with the OS, other configuration choices you have with VMs include:

- The size, which determines factors such as how many disks you can attach and the processing power. Azure offers a wide variety of sizes to support many types of uses.
- The Azure region where your new VM will be hosted, such as in the US, Europe, or Asia.

### 4.2 Availability Sets

With the exception of specific VMs that use premium storage, individual VMs within Navisite do not have availability SLAs; instead SLAs are provided on multiple VMs that can then be configured at an application level for redundancy. A simple example would be that of identical web servers that are set behind a load balancer such that a web request could go to any of them and return the same result. These VMs would be placed in an availability group by Navisite to ensure that during the course of routine maintenance, only one VM in the groups is rebooted at a time. This ensures continuous service while retaining the ability of Navisite and Microsoft to perform maintenance in a timely fashion.

### 4.3 VM Storage

![Azure Storage Concepts Diagram]
A standard storage account gives you access to Blob storage, Table storage, Queue storage, and File storage:

- **Blob Storage** stores file data. A blob can be any type of text or binary data, such as a document, media file, or application installer. Blob Storage is sometimes referred to as Object storage.
- **Table Storage** stores structured datasets. Table storage is a NoSQL key-attribute data store, which allows for rapid development and fast access to large quantities of data.
- **Queue Storage** provides reliable messaging for workflow processing and for communication between components of cloud services.
- **File Storage** offers shared storage for legacy applications using the standard SMB protocol. Azure virtual machines and cloud services can share file data across application components via mounted shares, and on-premises applications can access file data in a share via the File service REST API.

Azure Premium Storage delivers high-performance, low-latency disk support for virtual machines running I/O-intensive workloads. Virtual machine (VM) disks that use Premium Storage store data on solid-state drives (SSDs). You can migrate your application's VM disks to Azure Premium Storage to take advantage of the speed and performance of these disks.

An Azure VM supports attaching several Premium Storage disks so that your applications can have up to 64 TB of storage per VM. With Premium Storage, your applications can achieve 80,000 IOPS (input/output operations per second) per VM and 2000 MB per second disk throughput per VM with extremely low latencies for read operations.

When you provision a disk against a Premium Storage account, how much input/output operations per second (IOPS) and throughput (bandwidth) it can get depends on the size of the disk. Specific information about premium storage options can be found at https://azure.microsoft.com/en-us/services/storage/.

At this time, Navisite is only supporting Blob Storage for the VHD files as well as Premium Storage for VMs. Other storage formats may be made available at a later time.

### 4.4 Standalone Storage

Azure Storage as a Service (Azure Storage) is the simple presentation of bulk storage across the Internet without the need for VPNs or other special connectivity. Within Azure documentation it is referred to as blob storage. Rather than using storage protocols such as CIFS or NFS for transport, it uses HTTPS for dependable and secure data transfer. This means that it cannot be accessed natively by servers, but rather needs a specialized client to convert the storage protocol to HTTPS and back. More information can be found at https://azure.microsoft.com/en-us/services/storage/blobs/.

As a plentiful form of cheap storage, it is largely used for archiving or as a backup target. Many backup vendors (Commvault and Veritas) or storage providers (NetApp) can natively use Azure blobs as a target without the need for extra software. For those who just want a simple client for mapping a file share, a simple Google search will turn up a variety of free or low cost clients that may meet the specific needs of the customer.
Azure blobs provide a variety of configuration options:

a. Location – This can be at any of the locations listed in Services link above where Navisite is permitted to sell Azure.

b. Redundancy – Navisite encourages either the Locally Redundant Storage (three copies within one region) or Geo Redundant Storage (three copies within one region and three copies in another region generally in the same political border). GRS is roughly twice the price of LRS but provides an extra layer of redundancy at a relatively low cost.

c. “Hot versus Cool” – These are differentiated by SLA; Hot has a 99.9% SLA while Cool is 99%, but Cool is cheaper. More information can be found at https://docs.microsoft.com/en-us/azure/storage/storage-blob-storage-tiers

4.5 Networking

An Azure virtual network (VNet) is a representation of a physical network in the cloud; it is a logical isolation of the Azure cloud dedicated to an individual customer subscription. This allows for Navisite to define and control the IP address blocks, DNS settings, security policies, and route tables within this network. V Nets can be further segmented into subnets and launch Azure IaaS virtual machines. Additionally, the virtual network can be connected to on-premises network using one of the connectivity options available in such as VPN or Express Route.

The Azure infrastructure takes on the role of the router, allowing access from the VNet to the public Internet without the need of any configuration. Firewalls can be substituted by Network Security Groups (NSGs) applied to each individual subnet. Traditional physical load balancers are substituted by internet facing and internal load balancers in Azure.

4.5.1 Virtual Network Benefits

- V Nets are completely isolated from one another. That allows you to create disjoint networks for development, testing, and production that use the same CIDR address blocks.
- All IaaS VMs and PaaS role instances in a VNet can access the public Internet by default. Navisite can control access by using Network Security Groups (NSGs).
- PaaS role instances and IaaS VMs can be launched in the same virtual network and they can connect to each other using private IP addresses even if they are in different subnets without the need to configure a gateway or use public IP addresses.
- Azure provides internal name resolution for IaaS VMs and PaaS role instances deployed in your VNet. Navisite can also deploy DNS servers and configure the VNet to use them.
- Traffic entering and exiting the virtual machines and PaaS role instances in a VNet can be controlled using Network Security groups.
- V Nets can be connected to each other, and even to your on-premises datacenter, by using a site-to-site VPN connection, or ExpressRoute connection.
4.5.2 Subnets
Subnet is a range of IP addresses in the VNet; Navisite can divide a VNet into multiple subnets for organization and security. VMs and PaaS role instances deployed to subnets (same or different) within a VNet can communicate with each other without any extra configuration. Navisite can also configure route tables and NSGs to a subnet.

4.5.3 IP addresses
There are two types of IP addresses assigned to resources in Azure: public and private. Public IP Addresses allow Azure resources to communicate with the Internet and other Azure public-facing services like Azure Redis Cache, Azure Event Hubs. Private IP Addresses allows communication between resources in a virtual network, along with those connected through a VPN, without using an Internet-routable IP addresses.

4.5.4 Azure load balancers
Virtual machines and cloud services in a Virtual network can be exposed to the Internet using Azure Load balancers. Line of Business applications that are internal facing only can be load balanced using internal load balancer.

- An external load balancer can provide high availability for IaaS VMs and PaaS role instances accessed from the public Internet.
- An internal load balancer can provide high availability for IaaS VMs and PaaS role instances accessed from other services in a VNet.
4.5.5 Azure Traffic Manager

While basic load balancers provide sufficient functionality for distributing loads within a single location, there are frequently scenarios where the need exists to distribute loads between different geographies; for this Azure Traffic Manager can be used. Traffic Manager provides geographic load balancing by allowing requests to be distributed based on:

- Prioritized Routing – An algorithm primarily used in failover scenarios.
- Weighted Routing – An algorithm that allows for distribution to different hosts based on pre-defined priorities.
- Performance Routing – An algorithm that selects the best route based on latency between the source IP and the hosts.
- Geographic Routing – An algorithm that defines hosts based on the geographic region from whence the DNS query originates.

Each of these methods can be used based on the specific customer requirement. Two important points to note with Traffic Manager are:

1. Traffic Manager provides DNS resolution, not active routing, so once Traffic Manager determines the host to which a client should connect, that traffic goes straight from client to host without needing to re-enter the Azure environment.
2. Traffic Manager can be used to distribute traffic between hosts both within and outside of Azure. This allows for load balancing between Azure and other environments during a migration or “cloud bursting” scenario.

The following is a sample scenario for using Traffic Manager to do load balancing based on the performance algorithm:
4.5.6 Network Security Group (NSG)
Network security group (NSG) contains a list of Access control List (ACL) rules that allow/deny network traffic to your VM instances in a Virtual Network. NSGs can be associated with either subnets or individual VM instances within that subnet. When a NSG is associated with a subnet, the ACL rules apply to all the VM instances in that subnet. In addition, traffic to an individual VM can be restricted further by associating a NSG directly to that VM.

4.5.7 Routing
With user defined routes, Navisite has complete control over the traffic flow in each virtual network. Virtual network by default provides system routes for traffic flow between virtual machines. Navisite can customize the routing table by defining routes allowing specific traffic through network appliances. Routes can be defined in a routing table and applied to subnets. Every VM within a subnet automatically inherits the routes from the routing table. A route within the routing table contains the network address space (destination prefix) and the IP address of the next hop. You can also choose to bring in routes using BGP when using ExpressRoute. Within the routing table, a route for a given destination will be selected based on Longest Prefix match (LPM).
4.5.8 VPN Gateways

VPN Gateways are used to send network traffic between virtual networks and on-premises locations. They are also used to send traffic between multiple virtual networks within Azure (VNet-to-VNet). There are 3 VPN Gateway SKUs (Basic/Standard/High Performance) and Navisite will select the most appropriate one based on client requirements.

4.5.9 Express Route

For those customers who require dedicated connectivity to an Azure environment, Express Route can be used. An Express Route connection has three major components:

- The circuit that connects the customer premise to a carrier hotel. Most major telco providers offer this service with connectivity to Azure (Express Route) and AWS (Direct Connect). Navisite cannot directly resell these circuits so they should be obtained by the customer or through Spectrum Enterprise.
- A carrier hotel is an aggregation point for connecting customer circuits into the Azure network. There are some telco providers who provide this service directly while others will partner through speciality providers such as Equinix.
- The actual Express Route connection is effectively a cross-connect within the carrier hotel and the customer Azure subscription. This is configured by Navisite using routing and other configuration information supplied by the customer and carrier hotel.

4.6 License Models

Microsoft provides three different models for the acquisition and payment of Azure services; Pay-as-you-go, Enterprise Agreements, and Cloud Service Providers. Navisite can provide management services on top of all of these models, but there are slight differences in the approach.

- Pay-as-you-go is a model wherein a customer signs up for an account directly on the Microsoft portal and pays directly by credit card or invoice. This is most common among small companies or startups. Navisite can manage some or all of the Azure resources based on customer requirements.
• Enterprise Agreements for large Microsoft customers will frequently include some quantity of Azure credits in addition to the onsite Microsoft licenses. These are generally paid for in advance and this model is generally targeted to mid-to-large customers with a pre-existing Microsoft relationship. Navisite can manage some or all of the Azure resources based on customer requirements.
• The Cloud Service Provider program allows providers like Navisite to provide both the Azure resources and the Azure management in a single package. All Azure resources provided via this model must be managed by Navisite.

5. SERVICE DESCRIPTION
Navisite’s Managed Azure is a comprehensive managed hosting service that provides the following service components:

• Provisioning of VMs and networking components based on customer requirements
• Provisioning and management of backups for the Azure-hosted services
• Provisioning and management of Load Balancing services for the Azure-hosted services
• Availability Monitoring, Incident Management, System Administration, and Change Management Technical Support services for network connectivity and operating system.
• Access to Proximity customer portal.

5.1 Service Availability
Navisite’s Managed Azure service is available at all Azure locations as listed at https://azure.microsoft.com/en-us/regions/ for Pay-as-you-go and Enterprise Agreement models; only a subset of those regions are available through CSP.

5.2 Design Document Creation
The initial step is the joint creation of an environment design document (Design) by the Navisite sales and engineering teams with final approval by the customer. This Design will be based on pre-defined Navisite templates to ensure that configurations meet minimum requirements for service and support. The final document will include:

• Detailed description of network connectivity to the customer premise, Navisite hosted services, or other locations
• List of applications to be implemented with connectivity requirements
• List of Azure services to be used
• Specifications for Availability groups
• Geographic location for each availability group

Navisite strongly encourages the use of Availability groups when deploying VMs, but will pass-through the reduced Microsoft SLA on standalone VMs provided that they utilize premium storage.
5.3 Provisioning of Microsoft Azure account
For CSP customers, Navisite will provision an account on Azure for the customer; if the customer already has an Azure subscription, a separate process will be used to grant Navisite access to the existing account. This will serve as the basic environment into which all services will be deployed.

5.4 Network implementation
Navisite will provision the software-based network structure in based on the customer-approved design. Connectivity to the customer premise or Navisite hosted services will be provisioned and tested based on the Design document. This will include the configuration of a VPN or Express Route connection depending on specific customer needs.

5.5 DNS Implementation
Navisite will provision Azure DNS services and maintain both forward and reverse name lookup records for servers hosted within the Azure or Navisite environments.

5.6 Availability Group/Virtual Machine implementation
Navisite will create the appropriate resource and availability groups to support the Design. Within those groups, Navisite will provision the individual VMs and harden the operating systems of the in accordance with the approved network design as well as best practices and industry standards. Navisite is responsible for:

- Disabling unnecessary services as security measures.
- Installing and configuring TCP wrappers on UNIX hosts.
- Creating and configuring local user accounts

Customer may not reconfigure or re-install managed software associated with the Managed Azure service (i.e. remove or alter a monitoring agent, alter or change administrative accounts, change kernel parameters, system directory structure, or disk partition structure, etc.). Any of the above actions will void any associated SLA. Restoration of the OS parameters to the last supported build will be performed on a chargeable time and materials basis. Management of Customer environments using the Customer’s own server image will require prior approval on an individual case-by-case basis.

5.7 Blob Storage Implementation
Upon receipt of a sales order for Azure Storage, Navisite will:

a) Create an Azure subscription for the customer.
b) Create Resource Groups for tracking and management of the storage.
c) Create Storage Accounts based on the geographies requested by the customer.
d) Create Storage Blobs within the Storage Accounts based on the customer requirements.
e) Share the credentials and access keys required for accessing the storage blobs with the customer.

5.8 Load Balancer Implementation

In order to provide a unified interface for VMs located within an availability group, Load Balancer services are configured to provide access to services on the VMs. The load balancing services will be configured in accordance with the Design with the following parameters:

- Backend pool of VMs to be protected
- IP address for unified access
- Health probe configurations to determine whether or not a VM is live
- Load balancer rules (port/protocol)
- Inbound NAT rules (port mapping)
- Session persistence
- Global Load Balancing algorithm (Traffic Manager)

Upon successful configuration of the load balancing service, individual VMs will be shutdown to ensure that load balancing functionality occurs as expected.

5.9 Backup Implementation

Navisite utilizes our Unified Backup platform for backing up Azure VMs. Please see the Unified Backup SLD for more information.

5.10 Azure Import/Export Service

For those customers who have large quantities of data to be loaded into Azure, it may be more efficient to send data via magnetic media than sending it over a network. For these scenarios, Azure’s Import/Export service can be used. Navisite will provide the customer with necessary account information and then the customer can download the Import/Export tool and use it in accordance with Microsoft online documentation.

5.11 Implementation of the Navisite Monitoring platform

Navisite will add all Azure components to the Navisite monitoring platform. Alerts and general information from the Azure environment will be displayed within the client account in Proximity.
6. MONTHLY SERVICE DESCRIPTION

6.1 Design Updates

As customer requirements change over time, the environment may need to change from the original design as well. The customer is able to request changes to any Azure components via the Change Request form within Proximity. These changes will be validated and executed in accordance with Navisite change control processes.

6.2 OS Monitoring Services

Navisite assumes responsibility for the monitoring of the Customer’s operating systems. These operating systems are monitored 365 days a year, 24 hours a day to ensure that they are functioning as intended. Navisite initiates the notification process when a monitored threshold is reached or a fault is detected in the Customer infrastructure environment.

NOTE: Navisite reserves the right to change its monitoring tools, methods, monitored parameters, and polling intervals on an as needed basis.

6.2.1 Navisite Responsibilities / Activities

Network Monitoring

Navisite’s Network Management Platform performs the following functions:

- 24x7 ping monitoring of Customer servers or virtual instances to determine if they are in an Up or Down state.
- The Network Management Platform sends all confirmed error events to the Event Console in the Navisite Service Center (NSC) for further Event Management.

Navisite provides continuous, threshold-based monitoring of key critical parameters of the supported operating systems and server hardware to support availability. The NSC is notified if the thresholds for the critical parameters are exceeded; these “events” are then handled through Navisite’s Event Management process. Navisite provides key server performance statistics such as CPU utilization, Memory utilization, Swap space on the NaviView portal.

6.3 Network Management

Navisite will monitor and maintain the connectivity from the Azure environment to the customer or Navisite locations in accordance with the design or design changes. Modifications to Active Directory or DNS services will be requested via the Change Request form in Proximity and will be subject to Change Control processes.
6.4 OS Management Service

The Operating System (OS) Management Service consists of the following ongoing tasks:

- Ongoing Operational Management.
- Fault Management.
- Patch Management.
- Backup Services.

6.4.1 Ongoing Operational Management

Navisite continues to maintain the same operating system until the OS vendor no longer supports that version of the OS or until Navisite, with 6 month advance notice, advises Customers that, as a result of operational and/or security deficiencies, Navisite is removing the version from the Navisite list of supported service elements. Customers may need to provide or pay for any required upgrade licenses from the OS vendor.

Navisite Systems Administrators provide the following functions:

- Install/de-install OS packages, patches and service packs.
- Install and configure SSH for secure access to UNIX/LINUX servers.
- Add/change/delete local user accounts.
- Change/modify file permissions (read/write/execute commands and user access).
- Create file shares on Windows Servers.
- Keep Anti-virus engine and data files up to date.
- Modify system parameters in accordance with documented application requirements.
- Perform changes to TCP Wrappers to enable user access to UNIX hosts.
- Keep current with the operating system vendors' latest releases of security maintenance code patches. Subject to Customer notification and approval, Navisite periodically integrates the vendors’ latest security patches into production servers.

6.4.2 Fault Management

Navisite provides ongoing real-time monitoring of critical system parameters that are supported by proactive intervention by our System Administrators. We monitor and manage the Operating Systems as described above.

6.4.3 Windows Patch Management

Navisite is responsible for timely applications of vendor issued patches and service packs; these updates address performance and/or security issues. Navisite’s processes regarding the identification, testing, and deployment of OS patches is as follows:
6.4.3.1 Emergency patch procedures for security related issues

- Navisite monitors vendor alerts, trusted third party advisories, vulnerability reports, and other sources to identify valid security alerts/issues.

- Navisite installs emergency security patches immediately onto a Customer’s server if the patch is deemed so important by the vendor, or by industry experts, such that without it either the Customer or the Navisite network – and other Customers’ service elements – are exposed to attacks, which threaten their operational integrity. Navisite makes a reasonable attempt to notify affected Customers prior to patch installation (either via email or by phone), but in some circumstances it may be deemed necessary to install these patches before Customer notification occurs. Navisite also makes a reasonable effort to perform this emergency maintenance in the closest available regularly scheduled maintenance window, but in some cases action may be needed immediately.

- Navisite’s back out plans for emergency patch applications include being able to roll back to the current state of the OS prior to patch application. Any additional restoration of OS functionality, application information, or Customer data that may be necessary due to a security issue is provided under the Unified Backup Service. Refer to the Unified Backup Service SLD for further details.

6.4.3.2 Non-Emergency patch procedures for performance related issues

- Using vendor alerts, third party advisories, vulnerabilities reports, and other feedback, patches are collected as they become available, tested, and validated against the Navisite baseline OS system build.

- Periodically, but at least once a month, Navisite publishes a list of recommended patches and bundles these patches together in preparation for installation as a Mandatory System Patch Upgrade (MSPU). In addition, this list will be available to our Customers (as either the actual patch or a link to the patch) so that our Customers can review the patch list and determine by their own testing that the patches don’t affect their system or application’s operation.

- Approximately once every quarter Navisite publishes all the patches (or combined major Service Pack or service rollup) that are part of the next MSPU.

- Installation of each MSPU is implemented under a scheduled change control with the Customer given 14-day advance notification of the schedule for the change control and at least 28-day advance notification of the contents of the MSPU.
6.4.4 Linux Patch Management

Due to the greater number of inter-dependencies between Linux software packages and the applications that run on top of the operating system, Linux hosts are not patched on a regular schedule in the same manner as a Windows server. Navisite will apply operating system patches to a Linux machine under the following circumstances:

- An advisory has been posted for a security flaw in a well-known software module that places a server at undue risk of exploitation within the other security controls placed on a Navisite environment.
- There are specific requirements from an operating system or application vendor to apply a patch to fix a problem being experienced on the machine. This will be done after consultation with the client.
- A client specifically asks for patches to be applied.

6.4.5 Customer responsibilities:

- Refrain from making any changes to the operating system or any other element that is managed by Navisite. Navisite, in turn, will not make any changes to any elements managed by Customer.
- Notify the Navisite Service Center (NSC) prior to making any changes that may cause any unnecessary monitoring alarms. Troubleshooting and correcting any alarms caused by Customer’s failure to notify Navisite in advance will be billed against the monthly number of support hours.
- Ensure compatibility of Customer maintained applications with operating system, server hardware, and architecture.
- Request application of non-critical patches.

**NOTE:** For urgent vulnerabilities / critical patches, communication will be sent to the Customer indicating Navisite’s intent to patch their system unless instructed not to do so. If the Customer asks for a postponement, all systems are required to be patched within 30 days. If Customer refuses to allow Navisite to patch within 30 days, Customer will be required to execute an amendment to the SLA releasing Navisite of all responsibility.

6.5 Blob Storage Management

If a customer has trouble with their connectivity to the storage blob, Navisite can confirm the accuracy of the access credentials and keys as well as resetting them as necessary.

6.6 Load Balancer Management

Navisite will monitor the load balancer services to ensure that it continues to function as intended. In the event of an issue that renders one of the VMs unavailable, Navisite will
remediate as per the processes described in the preceding section. Errors will with the load balancing service itself will be similarly remediated.

In the event that the customer wishes to make changes to the overall Design in a manner that requires modification of the backend pool or other load balancer configurations, these changes will be communicated and executed via the Navisite Change Control process.
## 7. RACI’s

### 7.1 Windows Systems management

<table>
<thead>
<tr>
<th>Task</th>
<th>Notes</th>
<th>Responsible</th>
<th>Accountable</th>
<th>Consulted</th>
<th>Informed</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Initial Hardening</strong></td>
<td>Configure in accordance with Navisite’s standards and approved Operating System deployment.</td>
<td>Navisite</td>
<td>Navisite</td>
<td>Customer</td>
<td>Customer</td>
</tr>
<tr>
<td><strong>Monitoring /Reporting</strong></td>
<td>Setup and verify monitoring to established Navisite backend devices. Verify graphs are being populated and backup of configuration is being sent to log server.</td>
<td>Navisite</td>
<td>Navisite</td>
<td>Customer</td>
<td>Customer</td>
</tr>
<tr>
<td><strong>Backup configuration/Management</strong></td>
<td>Install and configure enterprise level backup software per customer requirements</td>
<td>Navisite</td>
<td>Navisite</td>
<td>Customer</td>
<td>Customer</td>
</tr>
<tr>
<td><strong>Compliance</strong></td>
<td>Harden operating system to meet industry requirements of the customer.</td>
<td>Navisite</td>
<td>Customer</td>
<td>Navisite</td>
<td>Customer</td>
</tr>
<tr>
<td><strong>Antivirus Management</strong></td>
<td>Install and configure antivirus in accordance with Navisite’s approved applications.</td>
<td>Navisite</td>
<td>Navisite</td>
<td>Customer</td>
<td>Customer</td>
</tr>
<tr>
<td></td>
<td>Real time, scheduled, and custom scanning. RemEDIATE issues as necessary.</td>
<td>Navisite</td>
<td>Navisite</td>
<td>Navisite</td>
<td>Customer</td>
</tr>
<tr>
<td><strong>Patch Management</strong></td>
<td>Install and maintain operating system patch levels and service packs based on approved industry packages.</td>
<td>Navisite</td>
<td>Navisite</td>
<td>Customer</td>
<td>Customer</td>
</tr>
<tr>
<td><strong>Enhancements and Upgrades</strong></td>
<td>Configuring additional software components.</td>
<td>Navisite</td>
<td>Navisite</td>
<td>Navisite/Customer</td>
<td>Customer</td>
</tr>
<tr>
<td><strong>Documentation</strong></td>
<td>Documentation regarding all configuration items specific to customers design.</td>
<td>Navisite</td>
<td>Navisite</td>
<td>Customer</td>
<td>Customer</td>
</tr>
<tr>
<td><strong>User Account Management</strong></td>
<td>Navisite applies user accounts based on customer requires and server needs.</td>
<td>Navisite</td>
<td>Navisite</td>
<td>Customer</td>
<td>Customer</td>
</tr>
<tr>
<td><strong>Break/Fix</strong></td>
<td>Resolve customer issues based on testing and production.</td>
<td>Navisite</td>
<td>Navisite</td>
<td>Navisite/Customer</td>
<td>customer</td>
</tr>
</tbody>
</table>
## 7.2 Linux Systems management

<table>
<thead>
<tr>
<th>Task</th>
<th>Notes</th>
<th>Responsible</th>
<th>Accountable</th>
<th>Consulted</th>
<th>Informed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial Hardening</td>
<td>Configure in accordance with Navisite's standards and approved Operating System deployment.</td>
<td>Navisite</td>
<td>Navisite</td>
<td>Customer</td>
<td>Customer</td>
</tr>
<tr>
<td>Monitoring /Reporting</td>
<td>Setup and verify monitoring to established Navisite backend devices. Verify graphs are being populated and backup of configuration is being sent to log server.</td>
<td>Navisite</td>
<td>Navisite</td>
<td>Customer</td>
<td>Customer</td>
</tr>
<tr>
<td>Backup configuration/ Management</td>
<td>Install and configure enterprise level backup software per customer requirements.</td>
<td>Navisite</td>
<td>Navisite</td>
<td>Customer</td>
<td>Customer</td>
</tr>
<tr>
<td>Compliance</td>
<td>Harden operating system to meet industry requirements of the customer.</td>
<td>Navisite</td>
<td>Customer</td>
<td>Navisite</td>
<td>Customer</td>
</tr>
<tr>
<td>Antivirus Management</td>
<td>Install and configure antivirus in accordance with Navisite’s approved applications (hypervisor based).</td>
<td>Navisite</td>
<td>Navisite</td>
<td>Customer</td>
<td>Customer</td>
</tr>
<tr>
<td></td>
<td>Real time, scheduled, and custom scanning. RemEDIATE issues as necessary.</td>
<td>Navisite</td>
<td>Navisite</td>
<td>Navisite</td>
<td>Customer</td>
</tr>
<tr>
<td>Patch Management</td>
<td>Provide OS patch reporting and installation support.</td>
<td>Navisite</td>
<td>Navisite</td>
<td>Customer</td>
<td>Customer</td>
</tr>
<tr>
<td>Enhancements and Upgrades</td>
<td>Configuring additional software components.</td>
<td>Navisite</td>
<td>Navisite</td>
<td>Navisite/Customer</td>
<td>Customer</td>
</tr>
<tr>
<td>Documentation</td>
<td>Documentation regarding all configuration items specific to customers design.</td>
<td>Navisite</td>
<td>Navisite</td>
<td>Customer</td>
<td>Customer</td>
</tr>
<tr>
<td>User Account Management</td>
<td>Creation and management of Navisite administrator account and one customer administrator account.</td>
<td>Navisite</td>
<td>Navisite</td>
<td>Navisite</td>
<td>Customer</td>
</tr>
<tr>
<td>Break/Fix</td>
<td>Resolve customer issues based on testing and production.</td>
<td>Navisite</td>
<td>Navisite</td>
<td>Navisite/Customer</td>
<td>Customer</td>
</tr>
</tbody>
</table>