Security Management in Microsoft Azure

Abstract

Locking down systems that are used to control cloud IT operations is important in maintaining an infrastructure that meets security and compliance standards. This white paper discusses steps for enhancing remote management security while administering Microsoft Azure environments, including cloud services, Virtual Machines and custom applications.

Audience

This document is intended for IT pros and IT implementers. It will be most useful to individuals who are already familiar with how Microsoft Azure functions from a broad perspective, and who want to increase their knowledge of tools and processes for enhancing the security of Azure cloud management endpoints.

NOTE: Certain recommendations in this paper may result in increased data, network, or compute resource usage, and may increase your license or subscription costs.

Published November 2014

Table of Contents

1 Introduction

Microsoft Azure subscribers may have multiple points of access to manage their cloud environments, including management workstations, developer PCs and even privileged end-user devices that have task-specific permissions. In some cases, administrative functions are performed through web-based consoles such as the Azure management portal. In other cases, there may be direct connections to Azure from on-premises systems over Virtual Private Networks (VPNs), Terminal Services, client application protocols, or (programmatically) the Azure Service Management API (SMAPI). Additionally, client endpoints can be either domain joined or isolated and unmanaged, such as tablets or smartphones.

Although these multiple access and management capabilities provide a rich set of options, this variability can add significant risk to a cloud deployment, making it difficult to manage, track, and audit administrative actions. This variability may also introduce security threats through unregulated access to client endpoints that are used for managing cloud services. Using general or personal workstations for developing and managing infrastructure opens unpredictable threat vectors such as web browsing (e.g. watering hole attacks) or email (e.g. social engineering and phishing) as shown in Figure 1.

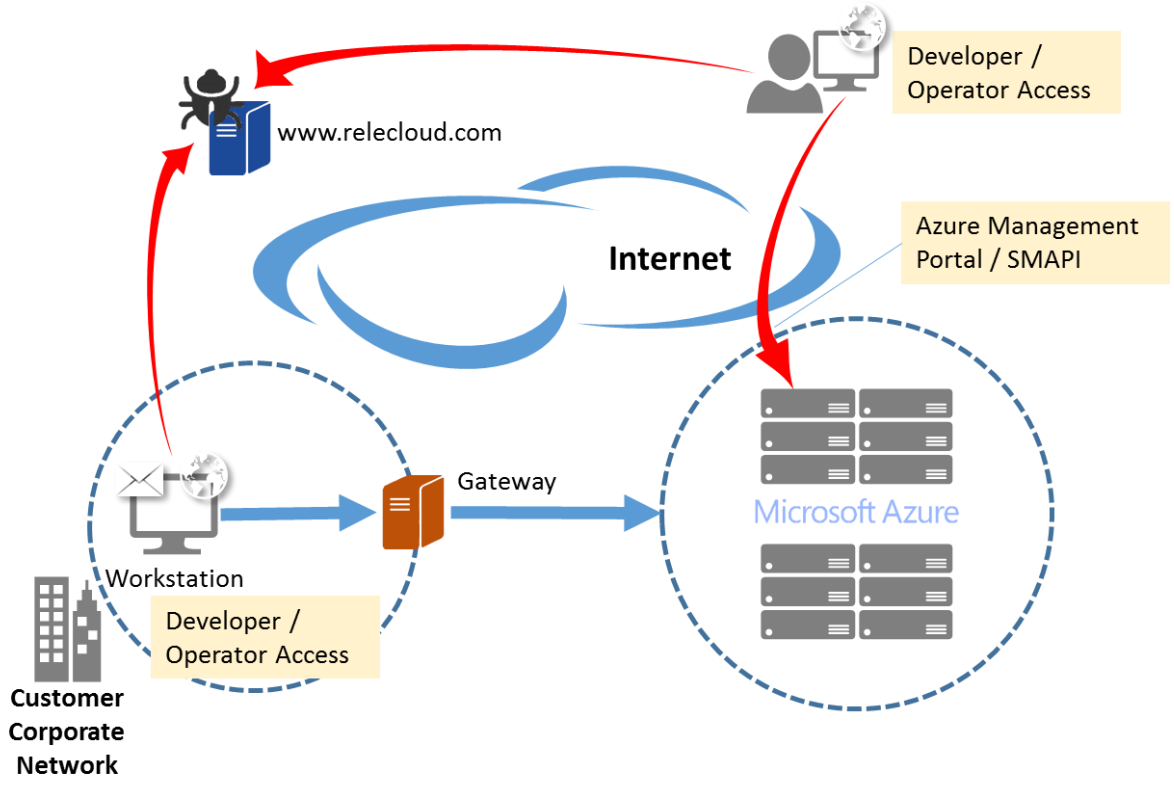

Figure 1: Typical management network topology.

The potential for attacks increases in this type of environment because it is challenging to construct security policies and mechanisms to appropriately manage access to Azure interfaces (such as SMAPI) from widely varied endpoints.

1.1 Remote Management Threats

A frequently used mechanism for attackers to gain privileged access involves breaching accounts by compromising account credentials (for example, through password brute forcing, phishing, and credential harvesting), or by tricking the users into running malicious code (for example, from malicious websites with drive-by downloads or from malicious email attachments). In a remotely managed cloud environment, account breaches can lead to an increased risk due to anywhere, anytime access.

Even with tight controls on primary administrator accounts, lower-level user accounts can be used to exploit weaknesses in one's security strategy. Lack of appropriate security training can also lead to breaches through accidental disclosure or exposure of account information.

When a user workstation is also used for administrative tasks, it can be compromised at many different points. Whether a user is browsing the web, using 3rd-party and open-source tools, or opening a malicious document file that contains a trojan.

In general, most targeted attacks that result in data breaches can be traced to browser exploits, plug-ins (such as Flash, PDF, Java), and spear phishing (email) on desktop machines. These machines may have administrative-level or service-level permissions to access live servers or network devices for operations when used for development or management of other assets.

1.2 Operational Security Fundamentals

As a rule for more secure management and operations, it is best to minimize a client's attack surface by reducing the number of possible entry points. This can be done through "separation of duties" and "segregation of environments" security principles: isolating sensitive functions from one another decreases the likelihood that a mistake at one level will lead to a breach in another. As such, administrative tasks should not be combined with activities that might lead to a compromise (for example, malware in an administrator's email that then infects an infrastructure server). Similarly, the workstation used for high-sensitivity operations should not be the same system used for high-risk purposes such as browsing the Internet.

Each application or service installed on an administrator's workstation increases security risks due to potential vulnerabilities that can be exploited. Therefore, reducing the system's attack surface by removing unnecessary software from a standard installation system image improves client manageability and stability, and hardens the client software security profile. For example, any standard administrative, support, or development workstation should not require installation of an email client or other productivity applications if the device's main purpose is to manage cloud services.

The network should treat client systems that have administrator access to infrastructure components as if they are as sensitive as the infrastructure components themselves. Since a compromise of an administrator or administrator system might lead to a service breach, the client should be subjected to the strictest possible policy to reduce security risks. Security policies that increase scrutiny on client devices

that possess administrative privileges can include Group Policy settings that deny open Internet access from the device and use of a restrictive firewall configuration.

You can implement other measures, including:

- Using Internet Protocol security (IPsec) VPNs if direct access is needed.
- Configuring separate management and development Active Directory domains.
- Isolating and filtering management workstation network traffic.
- Using antimalware software.
- Implementing multi-factor authentication to reduce the risk of stolen credentials.

Consolidating access resources and eliminating unmanaged endpoints also simplifies management tasks.

1.3 Providing Security for Azure Remote Management

Azure provides security mechanisms to aid administrators who manage Azure cloud services and virtual machines. These mechanisms include:

- Authentication and role based access control.
- Monitoring and logging (auditing).
- Certificates and encrypted communications.
- A web management portal.
- Network packet filtering.

In combination with client-side security configuration and datacenter deployment of a management gateway, it is possible to restrict and monitor administrator access to cloud applications and data.

2 Hardened Workstation for Management

The goal of hardening a workstation is to eliminate all but the most critical functions required for it to operate, making the potential attack surface as small as possible. System hardening includes minimizing the number of installed services and applications, limiting application execution, restricting network access to only what is needed, and always keeping the system up to date. Furthermore, using a hardened workstation for management segregates administrative tools and activities from other end-user tasks.

Within an on-premises enterprise environment, you can limit the attack surface of your physical infrastructure through dedicated management networks, server rooms that have card access, and workstations that run on protected areas of the network (for information on Microsoft physical datacenter security, please visit the Global Foundation Services web site). In a cloud or hybrid IT model, being diligent about secure management services can be more complex because of the lack of physical access to IT resources. Implementing protection solutions requires careful software configuration, security-focused processes, and comprehensive policies.

Using a least-privilege minimized software footprint in a locked-down workstation for cloud management—as well as for application development—can reduce the risk of security incidents by standardizing the remote management and development environments. A hardened workstation configuration can help prevent the compromise of accounts that are used to manage critical cloud resources by closing many common avenues used by malware and exploits. Specifically, you can use Windows AppLocker and Hyper-V technology to control and isolate client system behavior and mitigate threats, including email or Internet browsing.

On a hardened workstation, the administrator runs as a standard user (which blocks administrative-level execution) and associated applications are controlled by an allow list. The basic elements of a hardened workstation, as shown in Figure 2, are as follows:

- **Active scanning and patching**. Deploy antimalware software, perform regular vulnerability scans, and update all workstation by using the latest security update in a timely fashion.
- **Limited functionality**. Uninstall any applications that are not needed and disable unnecessary (startup) services.
- **Network hardening**. Use Windows Firewall rules to allow only valid IP addresses, ports, and URLs related to Azure management. Ensure that inbound remote connections to the workstation are also blocked.
- **Execution restriction**. Allow only a set of predefined executable files that

Figure 2: Fundamentals of a hardened workstation.

are needed for management to run (referred to as "default-deny"). By default, users should be denied permission to run any program unless it is explicitly defined in the allow list.

- **Least privilege**. Management workstation users should not have any administrative privileges on the local machine itself. This way, they cannot change the system configuration or the system files, either intentionally or unintentionally.

You can enforce all of this by using Group Policy Objects (GPOs) in Active Directory Domain Services (AD DS) and applying them through your (local) management domain to all management accounts.

2.1 Managing Services, Applications, and Data

Azure cloud services configuration is performed through either the Azure management portal or SMAPI, via the Windows PowerShell command-line interface or a custom-built application that takes advantage of these RESTful interfaces. Services using these mechanisms include Azure Active Directory (Azure AD), Azure Storage, Azure Websites, and Azure Virtual Network, among others.

Virtual Machine–deployed applications provide their own client tools and interfaces as needed, such as the Microsoft Management Console (MMC), an enterprise management console (such as Microsoft System Center or Windows Intune), or another management application—Microsoft SQL Server Management Studio, for example. These tools typically reside in an enterprise environment or client network. They may depend on specific network protocols, such as Remote Desktop Protocol (RDP), that require direct, stateful connections. Some may have web-enabled interfaces that should not be openly published or accessible via the Internet.

You can restrict access to infrastructure and platform services management in Azure by using multi-factor authentication, X.509 management certificates, and firewall rules. The Azure management portal and SMAPI require Transport Layer Security (TLS). However, services and applications that you deploy into Azure require you to take protection measures that are appropriate based on your application. These mechanisms can frequently be enabled more easily through a standardized hardened workstation configuration.

2.2 Management Gateway

To centralize all administrative access and simplify monitoring and logging, you can deploy a dedicated Remote Desktop Gateway (RD Gateway) server in your on-premises network, connected to your Azure environment.

RD Gateway is a policy-based RDP proxy service that enforces security requirements. Implementing RD Gateway together with Windows Server Network Access Protection (NAP) helps ensure that only clients that meet specific security health criteria established by AD DS GPOs can connect. In addition:

- Provision an Azure management certificate on RD Gateway so that it is the only host allowed to access the Azure management portal.

- Join RD Gateway to the same management domain as the administrator workstations. This is necessary when you are using a site-to-site IPsec VPN within a domain that has a one-way trust to Azure AD, or if you are federating credentials between your on-premises AD DS instance and Azure AD.
- Configure a client connection authorization policy to let the RD Gateway verify that the client machine name is valid (domain joined) and allowed to access the Azure management portal.
- Use IPsec for Azure VPN to further protect management traffic from eavesdropping and token theft, or consider an isolated Internet link via Azure ExpressRoute.
- Enable multi-factor authentication (via Azure Multi-Factor Authentication) or smart-card authentication for administrators who log on through RD Gateway.
- Configure source IP address restriction (IP address access control lists, firewall rules, and input endpoint port mappings) in Azure to minimize the number of permitted management endpoints.

2.3 Security Guidelines

In general, helping to secure administrator workstations for use with the cloud is very similar to the practices used for any workstation on-premises—for example, minimized build and restrictive permissions. Some unique aspects of cloud management are more akin to remote or out-of-band enterprise management. These include the use and auditing of credentials, security-enhanced remote access, and threat detection and response.

2.3.1 Authentication

You can use Azure logon restrictions to constrain source IP addresses for accessing administrative tools and audit access requests. To help Azure identify management clients (workstations and/or applications), you can configure both SMAPI (via customer-developed tools such as Windows PowerShell cmdlets) and the Azure management portal to require client-side management certificates to be installed, in addition to SSL certificates. It is also recommend that administrator access require multi-factor authentication.

Some applications or services that you deploy into Azure may have their own authentication mechanisms for both end-user and administrator access, whereas others take full advantage of Azure AD. Depending on whether you are federating credentials via Active Directory Federation Services (AD FS) or maintaining user accounts solely in the cloud, using Microsoft Forefront Identity Manager (part of Azure AD Premium) will help you manage identity lifecycles between the resources.

2.3.2 Connectivity

Several mechanisms are available to help secure client connections to your Azure virtual networks. Two of these mechanisms, site-to-site VPN and point-to-site VPN, enable the use of Network Access Protection (NAP), IPsec, and Layer Two Tunneling Protocol (L2TP). When Azure is connecting to public-facing Azure services management such as the Azure management portal, Azure requires Hypertext Transfer Protocol Secure (HTTPS).

A stand-alone hardened workstation that does not connect to Azure through RD Gateway should use IPsec or L2TP for its point-to-site VPN.

2.3.3 Management Auditing vs. Policy Enforcement

Typically, there are two approaches for helping to secure management processes: auditing and policy enforcement. Doing both will provide comprehensive controls, but may not be possible in all situations. In addition, each approach has different levels of risk, cost, and effort associated with managing security, particularly as it relates to the level of trust placed in both individuals and system architectures.

Monitoring, logging, and auditing provide a basis for tracking and understanding administrative activities, but it may not always be feasible to audit all actions in complete detail due to the amount of data generated. Auditing the *effectiveness* of the management policies is a best practice, however.

Policy enforcement that includes strict access controls puts programmatic mechanisms in place that can govern administrator actions, and it helps ensure that all possible protection measures are being used. Logging provides proof of enforcement, in addition to a record of who did what, from where, and when. Logging also enables you to audit and crosscheck information about how administrators follow policies, and it provides evidence of activities.

2.4 Client Configuration

We recommend three primary configurations for a hardened workstation. The biggest differentiators between them are cost, usability, and accessibility, while maintaining a similar security profile across all options. Table 1 provides a short analysis of the benefits and risks to each. (Note that "corporate PC" refers to a standard desktop PC configuration that would be deployed for all domain users, regardless of roles.)

CONFIGURATION	BENEFITS	CONS
STAND-ALONE HARDENED WORKSTATION	• Tightly controlled workstation • Reduced risk of application exploits • Clear separation of duties	• Higher cost for dedicated desktops • Increased management effort
CORPORATE PC AS VIRTUAL MACHINE	• Reduced hardware costs • Segregation of role and applications	
WINDOWS TO GO WITH BITLOCKER DRIVE ENCRYPTION	• Compatibility with most PCs • Cost-effectiveness and portability • Isolated management environment	• Asset tracking

Table 1: Comparison of hardened workstation configurations.

It is important that the hardened workstation is the Host and not the Guest, with nothing between the host operating system and the hardware. Following the "clean source principle" (also known as "secure origin") means that the Host should be the most hardened. Otherwise, the hardened workstation (Guest) is subject to attacks on the system on which it is hosted.

You can further segregate administrative functions through dedicated system images for each hardened workstation that have only the tools and permissions needed for managing select Azure and cloud applications, with specific local AD DS GPOs for the necessary tasks.

For IT environments that have no on-premises infrastructure (for example, no access to a local AD DS instance for GPOs because all servers are in the cloud), a service such as Windows Intune can simplify deploying and maintaining workstation configurations.

2.4.1 Stand-Alone hardened workstation for management

With a stand-alone hardened workstation, administrators have a PC or laptop that they use for administrative tasks and another, separate PC or laptop for non-administrative tasks. Thus, a workstation dedicated to managing your Azure services does not need other applications installed. Additionally, using workstations that support a Trusted Platform Module (TPM) or similar hardware-level cryptography technology aids in device authentication and prevention of certain attacks. TPM can also support full-volume protection of the system drive by using BitLocker Drive Encryption.

In the stand-alone hardened workstation scenario (shown in Figure 3), the local instance of Windows Firewall (or a non-Microsoft client firewall) is configured to block inbound connections, such as RDP. The administrator can log on to the hardened workstation and start an RDP session that connects to Azure, but cannot log on to a corporate PC and use RDP to connect to the hardened workstation itself.

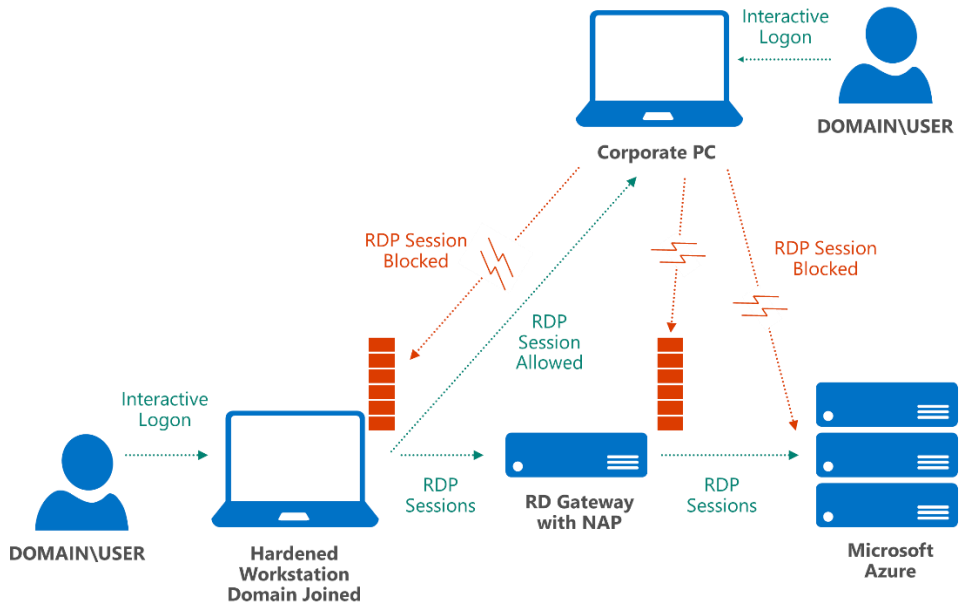

Figure 3: Topology for supporting a stand-alone hardened workstation.

2.4.2 Corporate PC as Virtual Machine

In cases where a separate stand-alone hardened workstation is cost prohibitive or inconvenient, the hardened workstation can host a Virtual Machine to perform non-administrative tasks (Figure 4).

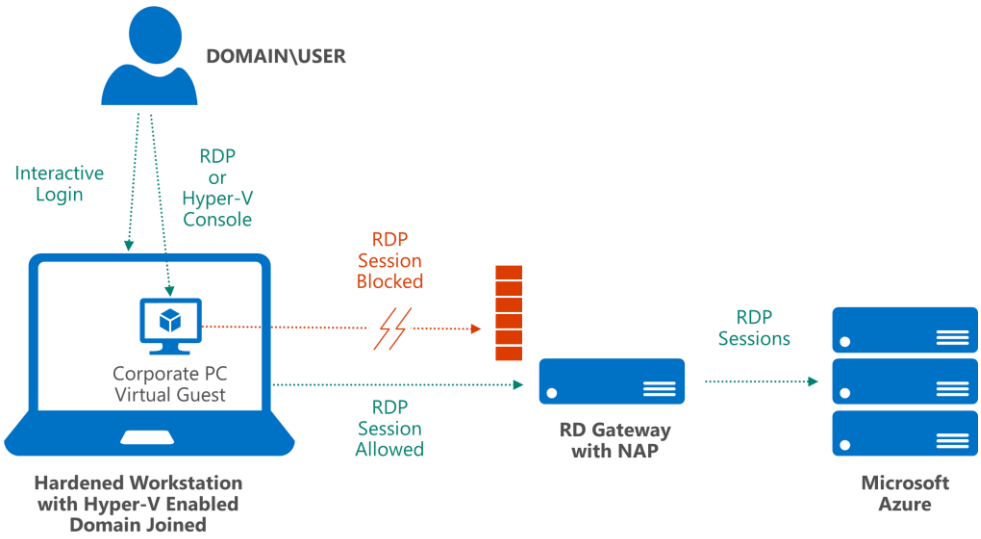

Figure 4: Topology for supporting a hardened workstation enabled with Hyper-V.

To avoid several security risks that can arise from using one workstation for systems management and other daily work tasks, you can deploy a Windows Hyper-V Virtual Machine to the hardened workstation. This Virtual Machine can be used as the corporate PC. The corporate PC environment can remain isolated from the Host, which reduces its attack surface and removes the user's daily activities (such as email) from coexisting with sensitive administrative tasks.

The corporate PC virtual machine runs in a protected space and provides user applications. The Host remains a "clean source" and enforces strict network policies in the root operating system (for example, blocking RDP access from the virtual machine).

2.4.3 Windows To Go

Another alternative to requiring a stand-alone hardened workstation is to use a Windows To Go drive, an available feature in Windows 8.1 Enterprise that supports a client-side USB-boot capability. Windows To Go enables users to boot a compatible PC to an isolated system image running from an encrypted USB flash drive. It provides additional controls for remote-administration endpoints because the image can be fully managed by a corporate IT group, with strict security policies, a minimal OS build, and TPM support.

In this approach (Figure 5), the portable image is a domain-joined system that is preconfigured to connect only to Azure, requires multi-factor authentication, and blocks all non-management traffic. If a user boots the same PC to the standard corporate image and tries accessing RD Gateway for Azure management tools, the session will be blocked. Windows To Go becomes the root-level operating system, and no additional layers are required (host operating system, hypervisor, virtual machine) that may be more vulnerable to outside attacks.

It is important to note that USB flash drives are more easily lost than an average desktop PC. Use of BitLocker to encrypt the entire volume, together with a strong password, will make it less likely that an attacker can use the drive image for malicious purposes. Additionally, if the USB flash drive is lost, revoking and issuing a new management certificate along with a quick password reset can reduce exposure. Administrative audit logs reside within Azure, not on the client, further reducing potential data loss.

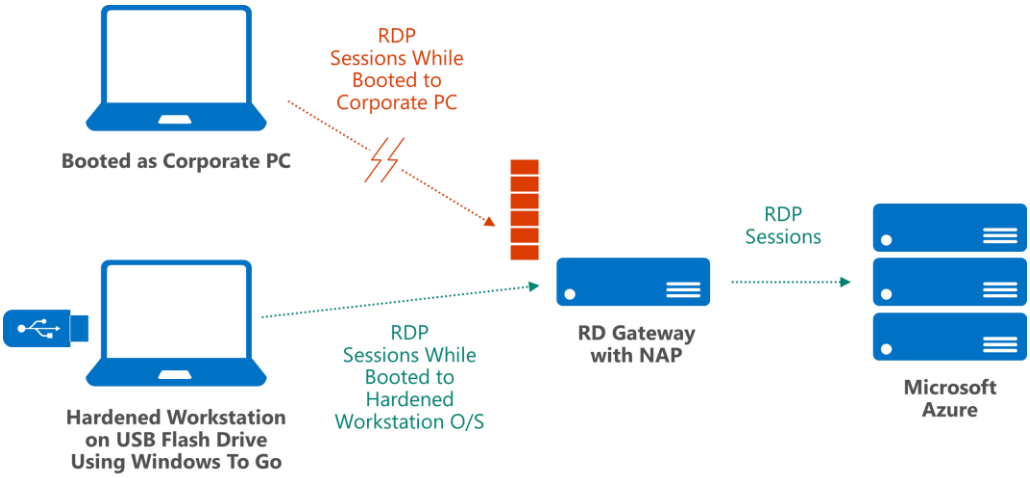

Figure 5: Topology for supporting a hardened workstation that uses Windows To Go on a USB flash drive.

3 Best Practices

Consider the following additional guidelines when you are managing applications and data in Azure.

3.1 Do's and Don'ts

Do not assume that because a workstation has been locked down that other common security requirements do not need to be met. Due to the elevated access levels that administrator accounts generally possess, the potential risk is much higher. Examples of risks and their alternate safe practices are shown in Table 2.

DO NOT	DO
Do not email credentials for administrator access or other secrets (e.g., SSL or management certificates).	Maintain confidentiality by delivering account names and passwords by voice (but not storing them in voice mail), perform a remote installation of client/server certificates (via an encrypted session), download from a protected network share, or distribute by hand via removable media. Proactively manage your management certificate life cycles.
Do not store account passwords unencrypted or un-hashed in application storage (such as in spreadsheets, SharePoint sites, or file shares).	Establish security management principles and system hardening policies, and apply them to your development environment. Use Enhanced Mitigation Experience Toolkit 4.1 certificate pinning rules to ensure proper access to Azure SSL/TLS sites.
Do not share accounts and passwords between administrators, or reuse passwords across multiple user accounts or services, particularly those for social media or other non-administrative activities.	Create a dedicated Microsoft account to manage your Azure subscription—an account that is not used for personal email.
Do not email configuration files.	Configuration files and profiles should be installed from a trusted source (for example, an encrypted USB flash drive), not from a mechanism that can be easily compromised, such as email.
Do not use weak or simple logon passwords.	Enforce strong password policies, expiration cycles (change-on-first-use), console timeouts, and automatic account lockouts. Use a client password management system with multi-factor authentication for password vault access.
Do not expose management ports to the Internet.	Lock down Azure ports and IP addresses to restrict management access. For more information, see the Azure Network Security white paper. Use firewalls, VPNs, and NAP for all management connections.

Table 2: Common security risks and mitigations.

3.2 Azure Operations

Within Microsoft's operation of Azure, operations engineers and support personnel who access Azure's production systems use hardened workstation PCs with VMs provisioned on them for internal corporate network access and applications (such as e-mail, intranet, etc.). All management workstation computers have TPMs, the host boot drive is encrypted with BitLocker, and they are joined to a special organizational unit (OU) in Microsoft's primary corporate domain.

System hardening is enforced through Group Policy, with centralized software updating. For auditing and analysis, event logs (such as security and AppLocker) are collected from management workstations and saved to a central location.

In addition, dedicated jump-boxes on Microsoft's network that require two-factor authentication are used to connect to Azure's production network.

3.3 Azure Security Checklist

Minimizing the number of tasks that administrators can perform on a hardened workstation will help minimize the attack surface in your development and management environment. Use the following technologies to help protect your hardened workstation:

- **IE hardening**. The Internet Explorer browser (or any web browser, for that matter) is a key entry point for malicious code due to its extensive interactions with external servers. Review your client policies and enforce running in protected mode, disabling add-ons, disabling file downloads, and using Microsoft SmartScreen filtering. Ensure that security warnings are displayed. Take advantage of Internet zones and create a list of trusted sites for which you have configured reasonable hardening. Block all other sites and in-browser code, such as ActiveX and Java.
- **Standard user**. Running as a standard user brings a number of benefits, the biggest of which is that stealing administrator credentials via malware becomes more difficult. In addition, a standard user account does not have elevated privileges on the root operating system, and many configuration options and APIs are locked out by default.
- **AppLocker**. You can use AppLocker to restrict the programs and scripts that users can run. You can run AppLocker in audit or enforcement mode. By default, AppLocker has an allow rule that enables users who have an admin token to run all code on the client. This rule exists to prevent administrators from locking themselves out, and it applies only to elevated tokens. See also Code Integrity as part of Windows Server core security.
- **Code signing**. Code signing all tools and scripts used by administrators provides a manageable mechanism for deploying application lockdown policies. Hashes do not scale with rapid changes to the code, and file paths do not provide a high level of security. You should combine AppLocker rules with a PowerShell execution policy that only allows specific signed code and scripts to be executed.

- **Group Policy**. Create a global administrative policy that is applied to any domain workstation that is used for management (and block access from all others), as well as to user accounts authenticated on those workstations.
- **Security-enhanced provisioning**. Safeguard your baseline hardened workstation image to help protect against tampering. Use security measures like encryption and isolation to store images, virtual machines, and scripts, and restrict access (perhaps use an auditable check-in/check-out process).
- **Patching.** Maintain a consistent build (or have separate images for development, operations, and other administrative tasks), scan for changes and malware routinely, keep the build up to date, and only activate machines when they are needed.
- **Encryption.** Make sure that management workstations have a TPM to more securely enable Encrypting File System (EFS) and BitLocker. If you are using Windows To Go, use only encrypted USB keys together with BitLocker.
- **Governance.** Use AD DS GPOs to control all of the administrators' Windows interfaces, such as file sharing. Include management workstations in auditing, monitoring, and logging processes. Track all administrator and developer access and usage.

4 Summary

Using a hardened workstation configuration for administering your Azure cloud services, Virtual Machines, and applications can help you avoid numerous risks and threats that can come from remotely managing critical IT infrastructure. Both Azure and Windows provide mechanisms that you can employ to help protect and control communications, authentication, and client behavior.

5 References and Further Reading

The following resources are available to provide more general information about Microsoft Azure and related Microsoft services, in addition to specific items referenced in this paper:

- Microsoft Azure home page—general information and links about Microsoft Azure
  - http://azure.microsoft.com
- Microsoft Azure Documentation Center—developer guidance and information
  - http://azure.microsoft.com/en-us/documentation/
- Microsoft Azure Trust Center
  - http://azure.microsoft.com/en-us/support/trust-center/
- Microsoft Security Response Center—where Microsoft security vulnerabilities, including issues with Microsoft Azure, can be reported
  - http://www.microsoft.com/security/msrc/default.aspx
  - Or via email to secure@microsoft.com
- "New Guidance to Mitigate Determined Adversaries' Favorite Attack: Pass-the-Hash"
  - http://blogs.technet.com/b/security/archive/2012/12/11/new-guidance-to-mitigate-determined-adversaries-favorite-attack-pass-the-hash.aspx
- "How to Setup Windows Azure (Server 2012) as an SSTP and L2TP VPN Provider"
  - http://blogs.msdn.com/b/notime/archive/2013/06/01/how-to-configure-windows-azure-server-2012-as-an-sstp-vpn-provider.aspx