Table of Contents

RPS Security

The information below has been verified on the RPS 3.1, which shipped from Microsoft in Spring of 2020.

Ports and Protocols

RPS uses various ports and protocols for operation. Some ports are configurable as part of the RPS deployment and configuration, and some are outside the management of RPS and/or not configurable. The table below shows these RPS components (where * Indicates port is configurable via RPS).

Table 1: RPS Ports and Protocols

COMPONENT	DESCRIPTION	PORTS	PROTOCOLS
RPS API	Direct management of configuration data in SQL Server	1433	TCP (TLS 1.2)
RPS Sync Service	Synchronize Data and Static Files between RPS Nodes and managed RPS Targets	777*	HTTPS
DFSR	Transfers files between nodes within a domain	445, 135	RPC, TCP
BITS	Transfers files between nodes on different domains	80, 443	HTTP/S
RPS Web	Administrative Website for RPS	8080*	HTTPS
RPS Provisioning Service	Baremetal/iPXE Service via the specific DNS name **rpsprovisioning**	443*	HTTPS
SMA	Service Management Automation	9090	HTTPS
TER Reader	Trust Element Repository – Reader (DCA)	3443	TCP
TER Writer	Trust Element Repository – Writer (DCA)	5443	TCP
WinRM	Windows Remote Management	5985/5986	HTTP/HTTPS
SMB	File Sharing	445	SMB/HTTPS
ICMP	Device Availability		ICMP
DHCP	Dynamic Host Configuration Protocol	67-69	UDP
DNS	Domain Name Server	53	UDP/TCP

Host-Based Security System (HBSS) uses some common ports (e.g., ports 80, 443, 1433, etc.) though requires additional ports be used for full operation. Please see HBSS documentation, at https://kc.mcafee.com/corporate/index?page=content&id=KB66797.

Service Accounts

The following accounts are used by RPS for setup and maintenance of Nodes.

RPS Account Roles: Domain Accounts

Table 2: Domain Accounts

ACCOUNT (ROLE)	DESCRIPTION	PERMISSIONS
DomainAdmin	Has full control of the domain. Administrator rights on all domain controllers and member servers.	**AD:** DomainAdmin[1]
DomainJoin	Used to join computers to the domain. Rights are scoped specifically for that purpose.	**AD:** Force change password Read/Write Computers
ProvSvc	Provisioning Website App Pool Identity	**SQL:** Service Permissions[2]
GuiSvc	RPS Website App Pool Identity	**RPS:** Master Key Encryption **SQL:** Service Permissions[2]
SmaRunbookSvc	SMA Runbook	**RPS:** Master Key Encryption **SQL:** Service Permissions[2]
SmaWebSvc	SMA IIS App Pool	**SQL:** Service Permissions[2]
SqlAgentSvc	SQL Server Agent	**AD:** Log on as a Service
SqlSvc	SQL Server Service	**AD:** Log on as a Service **SQL:** DBOwner
SyncSvc	Sync Service Account	**AD:** Log on as a Service **SQL:** Service Permissions[2]

RPS Account Roles: Server Accounts

Table 3: Server Accounts

ACCOUNT (ROLE)	DESCRIPTION	PERMISSIONS
ServerAdmin	Push certificates and settings, manage DSC configuration, pull files from content store	AD Account w/ Local Admin
LocalAdmin	Manage machine settings for non-domain joined computer	Local Admin

RPS Account Roles: Other

Table 4: Other Accounts

ACCOUNT (ROLE)	DESCRIPTION	PERMISSIONS
SA	Account used to setup SQL. This account is disabled per STIG after setup is complete.	SQL

[1] Domain Administrator membership is required to create a new Domain Controller. After initial creation, the account should be removed from this group, but should still retain permissions to manage AD Users, Computers, Groups and OUs.

[2] Service SQL permissions are scoped to the RpsDb only and include Execute, Select, Insert, Update, Delete, and SyncHistory change tracking view permissions.

Security

Partial Configurations

All RPS Partial Configs must define the following parameters:

- **IPAddress** - Accessible IP Address of the computer we'll publish DSC Configuration to.
- **DSCEncryptionCertificate** - Information about the certificate used to encrypt the MOF (configuration). The LCM is set to use this certificate and any partials that are not secured will not run on a target.
- **OutputPath** - Location to temporarily store the MOF file once its compiled.

Runbooks

Many Runbooks will need to connect to the Target (Computer) to perform their duty. To connect, you must get the appropriate credential and then establish a secure connection. Runbooks use the `GetRpsCredential` cmdlet to load the right credential for the target; then use `New-SecureSession` from Rps-Api to make the connection.

Patching

Patch Management in RPS requires communication via HTTPS. The certificate authority (CA) that signed the webserver's certificate must be trusted by the Linux client or patches will not be downloaded. This is done by installing the public certificate of the CA.

Certificates

The RPS Solution uses certificates for a variety of functions, including:

- Web Site SSL binding for HTTPS encrypted transport between server (e.g., RPS Website) and client.
- RPS Sync Service for client\server authentication between **subscriber** (e.g., RPS Sync Service on Region) and **distributor** (e.g., RPS Sync Service on Master) nodes. The certificate thumbprints for all trusted nodes are whitelisted in the RPS CMDB.
- RPS Sync Service for HTTPS encrypted transport between server and client.
- DSC MOF file credentials encryption (By default DSC encrypts the entire MOF file).
- WinRM for HTTPS encrypted transport between server and client.
- SQL for HTTPS encrypted transport between server and client.
- Provisioning SSL binding for HTTPS encrypted transport between server (e.g., RPS Provisioning) and client.
- Encryption of secrets in the database (protected properties).
- Encryption of XML configurations.

Each certificate must be derived from a trusted root certificate that resides in the Trusted Root Certification Authorities store.

Table 5: Certificates

ROLE	DISTRIBUTION	KEY USAGES	PURPOSE
DscEncryption	Per VM	Key Encipherment, Data Encipherment (30)	MOF credential encryption
ProvisioningSSL	APP Master	Key Encipherment, Data Encipherment	HTTPS support for Provisioning Website
ClientCdn	Per VM		
FeedSSL			
GuiSSL	Per APP VM	Digital Signature, Non-Repudiation, Key Encipherment (e0)	HTTPS support for RPS GUI Website
iPxeSSL	Per APP VM	Digital Signature, Non-Repudiation, Key Encipherment (e0)	HTTPS support for iPXE Website
MasterKeyEncryption	Per Node		Protecting the Master Key

ROLE	DISTRIBUTION	KEY USAGES	PURPOSE
NodeEncryption	Per APP VM		Encrypting node configuration
Root	Per VM	Certificate Signing, Off-line CRL Signing, CRL Signing (06)	Deriving other certificates
Sync	Per APP VM		Allowing Sync to occur between nodes
SyncSSL	Per APP VM	Key Encipherment, Digital Signature, Non-Repudiation	Data-in-transit encryption for node sync
SqlSSL	Per APP VM		Data-in-transit encryption for SQL data
WinRM	Per VM		

Master Key

The Master Key (MK) is used to protect secrets in the database (i.e., credential/certificate passwords). Since the MK is high-value, it's encrypted using the public key of a certificate. Appropriate users are given access to the private key of the Master Key Encryption Certificate (MKEC) so that they may access the MK and decrypt protected properties in the database.

The same MK should be used for all nodes that will share secrets. The default boundary for secrets is an Active Directory domain since domain accounts will likely need access to all domain computers. This implementation is fungible, however any changes to the default implementation made by the customer/integrator may risk customer data.

Accounts which are preconfigured with the MasterKeyEncryption role during setup will have permissions to manipulate protected properties in the target environment. In order to give this permission to new users once RPS is installed, the role should be added to the appropriate account in the CMDB and DSC should be republished (at minimum, the RpsCertificate partial).

When a protected property is retrieved or set, access is determined by retrieving the MasterKeyCertThumbprint property on the node. If the user has access to the corresponding certificate private key in the LocalMachine\Personal store, they are granted access to the MK. If the user does not have rights to the MKEC, access to protected properties will be denied.