Table of Contents

RPS v4.0.0 Ports, Protocols, & Security Guide

Ports, Protocols, & Security Guide

Last updated on August 3, 2021.

Last Reviewed and Approved on PENDING REVIEW

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).

COMPONENT	DESCRIPTION	PORTS	PROTOCOLS
RPS API	Direct management of configuration data in PostgreSQL Server.	5432	TCP
RPS Sync Plugin	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	Bare-metal/iPXE Service via the specific DNS name **rpsprovisioning**.	443*	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

Table 1: RPS Ports and Protocols

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

Service Accounts

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

RPS Account Roles: Domain Accounts

ACCOUNT (ROLE)	DESCRIPTION	PERMISSIONS
DomainAdmin	Has full control of the domain. Administrator rights on all domain controllers and member servers.	**AD:** Domain Admin[1]
DomainJoinAdmin	Used to join computers to the domain. Rights are scoped specifically for that purpose.	**AD:** Force change password Read/Write Computers
ProvisioningServiceAccount	Provisioning Website App Pool Identity	**SQL:** Service Permissions[2]
GuiServiceAccount	RPS Website App Pool Identity	**AD:** Domain Admin[1] **RPS:** Master Key Encryption
SqlServiceAccount	SQL Server Service	**AD:** Log on as a Service
CdnServiceAccount	Has Access to the CDN folder.	CDN Folder, BITS Message Queue
DFSAdmin	Has minimum required permissions in Active Directory to manage DFSR.	**AD:** DFSR Management
MasterKeyEncryption	Users with this role will be granted read permissions to the MasterKey certificate private key.	Read Only
PluginClientAuth	Users with this role will get the RPS Web API client authentication certificates installed in their certificate store.	
WebApiServiceAccount	Account used to run the Web API service and Sync.	**AD:** Domain Admin[1] **SQL:** Service Permissions[2]
FileTransferServiceAccount	Account used to transfer files from ContentStore.	ContentStore NTFS permissions
DhcpServiceAccount	Account used to authorize DHCP.	DHCP Admin
DomainSchemaAdmin	Account used to extent the AD Schema and move domain controllers to different AD site.	**AD:** Schema Administrator, Domain Admin[1]
DomainUser	Account used to export certificates from Root and CA local machine certificate store (ClientPki.ps1).	Logon Permissions
TaskManagementServiceAccount	Domain level service account authorized to execute runbooks across the RPS domain.	**AD:** Domain Admin[1]
ServerAdmin	Push certificates and settings; manage DSC configuration; pull files from content store.	**AD:** Domain Admin[1]

Table 2: Domain Accounts

[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.

RPS Account Roles: Server Accounts

ACCOUNT (ROLE)	DESCRIPTION	PERMISSIONS
LocalAdmin	Manage machine settings for non-domain joined computer.	Local Admin
FileTransferServiceAccount	Account used to transfer files from ContentStore.	ContentStore NTFS permissions
VMWareAdmin	Account used for VMWare configuration.	VMWare Administrator
LocalAdminProvisioningOnly	Local Admin account, but only used for provisioning.	Local Admin

Table 3: Server Accounts

RPS Account Roles: Other

ACCOUNT (ROLE)	DESCRIPTION	PERMISSIONS
PostgreSqlSuperAccount	PostgreSQL administrative account.	SQL
DatabaseAccount	PostgreSQL account used by RPS to connect to the database.	SQL
DomainSafeModeAdmin	Account that credentials are used to create the Domain Controller DSRM password; only used in ADSitesAndSubnets.	

Table 4: Other Accounts

Security

Partial Configurations

All RPS partial configurations must define the following parameters:

- **IPAddress** - Accessible IP Address of the computer we will 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 it is compiled.

For additional information, refer to the RPS article Authoring RPS DSC Partial Configurations.

RPS Runbooks

Many RPS PowerShell 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 `Get-RpsCredential` or `Get-AdminRoleCredential` cmdlet to load the right credential for the target, then uses `New-SecureSession` from Rps-Api to make the connection.

For additional information, refer to the RPS article Authoring RPS Runbooks.

Patching

Patch Management in RPS requires communication via HTTPS. The certificate authority (CA) that signed the web server'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.

For additional information, refer to RPS Patching.

Certificates

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

- Website 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).
- Client Authentication for the DSC Pull Server.
- 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 in Certificate Manager on the RPS server(s).

ROLE	DISTRIBUTION	KEY USAGES	PURPOSE
DscEncryption	Per VM	Key Encipherment, Data Encipherment (30)	MOF credential encryption.
DscPullServer	Per VM	DigitalSignature, Client Authentication	DSC Pull Server Client Authentication
ProvisioningSSL	APP Master	Key Encipherment, Data Encipherment	HTTPS support for Provisioning Website.
RpsClientCdn	Per VM	Client Authentication	Patching Certificate Authentications.
RpsGuiSSL	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	Document Encryption, Key Encipherment, Data Encipherment	Protecting the Master Key.
NodeEncryption	Per APP VM	Document Encryption, Key Encipherment, Data Encipherment	Encrypting node configuration.
RpsRoot	Per VM	Certificate Signing, Off-line CRL Signing, CRL Signing (06)	Deriving other certificates.
RpsSync	Per APP VM	Client Authentication	Allowing Sync to occur between nodes.
RpsSyncSSL	Per APP VM	Key Encipherment, Digital Signature, Non-Repudiation	Data-in-transit encryption for node sync.
SqlSSL	Per APP VM	Server Authentication	Data-in-transit encryption for SQL data.
WinRM	Per VM	Server Authentication, Key Encipherment	Secure Connections to Targets.
CertificateApi	Per VM	Client Authentication	Certificate Manager API REST Certificate Client Authentication.

ROLE	DISTRIBUTION	KEY USAGES	PURPOSE
CertificateManager	Per VM	Client Authentication	Certificate API REST Certificate Client Authentication.
RpsAPi	Per VM	Client Authentication	RPS API REST Certificate Client Authentication.
RpsWebAPiSSL	Per APP VM	Digital Signature, Non-Repudiation, Key Encipherment (e0)	HTTPS Support for RPS Web API Host.
WindowActivation	All	Digital Signature	CA Chain to Activate Office and Windows.
WindowsActivationCA	All	Digital Signature, Certificate Signing, Offline CRL Signing, CRL Signing	CA Chain to Activate Office and Windows.

Table 5: Certificates

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 is 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 that 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\My 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.