On-Premise Solution (Appliance-X) Site Readiness Checklist

Version 2.3

Table of Contents

Introduction

The BlackBerry Workspaces on-premise solution enables organizations to securely share, sync, control, and track files among internal users and with partners and customers through software installed at the customer site.

This document provides a **mandatory checklist** for customers to verify that their site is prepared for the Appliance-X installation. It should be filled by the customer and returned to BlackBerry Professional Services prior to the deployment process. Proper site preparation is essential to ensure a smooth installation.

Prerequisites

The following section lists the prerequisites for BlackBerry Workspaces Appliance-X installation. Note that these prerequisites are the responsibility of the customer.

Virtualization Server

The customer must have an installed Virtualization platform, with capacity available to support the specifications as detailed in *Hardware Requirements*, section 7. Available platforms include, but are not limited to, ESX, ESXi, and Hyper-V. The customer may also choose to install the servers in their private Cloud environment such as Azure or AWS.

Domain Name & Branding

BlackBerry Workspaces installation requires clear identification of the domain name as well as the appropriate authorization certificates. The customer must provide BlackBerry Workspaces with the preferred FQDN (Fully qualified domain name; such as *workspaces.mycompany.com*). This address is branded into the Appliance and serves as the suffix of all URLs used to access the BlackBerry Workspaces services.

Certificates

The BlackBerry Workspaces Virtual Appliance must be provisioned with certificates that correspond to the domain where it is installed. **Since the core value of the product relies on its security, no self-signed certificates may be used, and only approved certificate authorities can sign the certificates.**

Please refer to the included Appendix for detailed SSL certificate requirements.

Mail Relay (SMTP) Identification

The BlackBerry Workspaces application uses email as part of standard operation. Therefore, an SMTP server must be specified for service to function.

NTP Server

Virtual Appliance installation requires precise timing synchronization. Both IP address and Hostname formats are supported.

Third-Party Licensing

As part of BlackBerry Workspaces' installation process, license activation for third party software is required. All licenses should be provided by the customer prior to installation. This software includes:

1. Microsoft products (Windows Server 2016 *and* Microsoft Office 2016 Standard/Pro edition)

2. Red Hat Enterprise Linux

App-X Installation Type	Third Party Software Licenses	Amount	Notes
Basic	Microsoft Windows Server 2016	1	
	Microsoft Office 2016 Standard/Pro edition	1	Standard, Professional, or Professional Plus
	Red Hat Enterprise Linux	1	RHEL Server license
Advanced	Microsoft Windows Server 2016	1+	Number of servers may vary. Consult with your PS Consultant
	Microsoft Office 2016 Standard/Pro	1+	1 license required for each 2016 server installed. Consult with your PS Consultant if there are questions
	Red Hat Enterprise Linux	4+	Number of servers may vary. Consult with your PS Consultant

Deployment Configuration

Architecture

The standard BlackBerry Workspaces virtual appliance solution is comprised of 2 virtual machines as detailed below. This deployment model is called *Appliance-X Basic*. For specialized deployments, or deployments which require High Availability, a larger scalable model is available called *Appliance-X Advanced*. Due to the varying nature of Appliance-X Advanced deployments, server count and specifications may vary. Therefore, please ask your Professional Services Consultant if you have any questions.

Appliance-X Basic

| Server Name	Responsibility
Main	Provide all end-user services, including database and file storage
Conversion - Windows	Convert Microsoft Office files to BlackBerry Workspaces secure formats
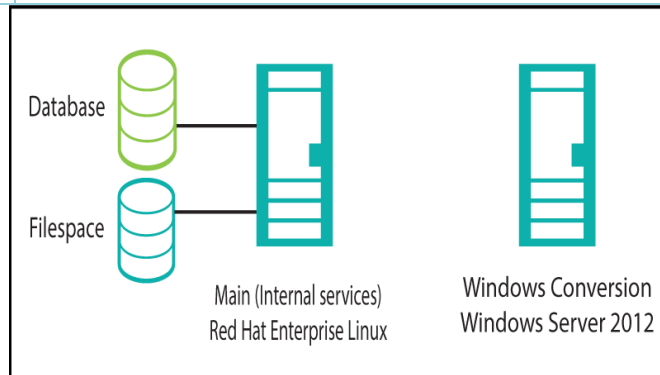
Appliance-X Advanced

Server name	Responsibility	Add copies of server for scale	Secondary copy of server for high availability
Orchestration	Deployment and configuration management		
Frontend	BlackBerry Workspaces application frontend & load balance end users between application resources. If you add a copy of the server for scale, an external load balancing solution is required.	✔	✔
Main	Internal appliance services, including database and file storage		✔
Application	BlackBerry Workspaces application, including web application and API service	✔	✔
Conversion - Windows	Converts Microsoft Office files to BlackBerry Workspaces secure format	✔	✔
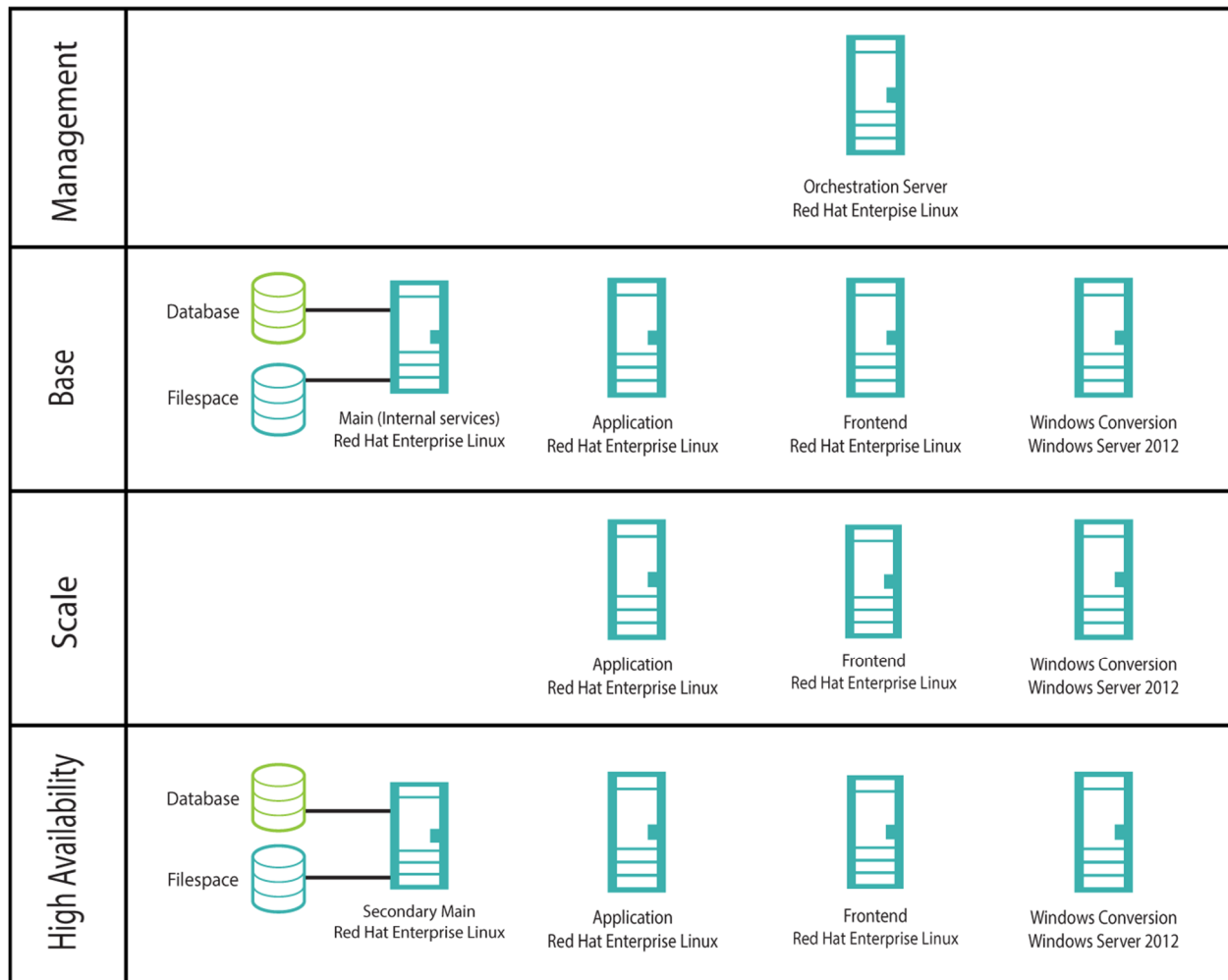
Checklist

1. **Network settings**	**Main RHEL IP:** ___.____.____.____ **Conversion Windows IP:** ___.____.____.____ **Network Mask:** ___.____.____.____ **Gateway:**

	___.____.____.____ **DNS 1:** ___.____.____.____ **DNS 2:** ___.____.____.____
2. **Please enter the name of the organization hosting the service, and the email address of the hosting service administrator.**	Hosting organization name: Click here to enter text. Administrator email address: Click here to enter text.
3. **Please enter the server's desired URL:** **Please note that this domain will require proper SSL certificates**	FQDN: Click here to enter text.
4. **Local server time-zone**	Click here to enter text.
5. **NTP server details**	IP or Hostname: Click here to enter text.
6. **SMTP server details**	Server IP: ___.____.____.____ Port (default 25): Click here to enter text. User (optional): Click here to enter text. Password (optional): Click here to enter text.
7. **How much space will be dedicated to the server for storage of end users' documents?** • **Note: Please plan for 20% overhead to this number for database storage. Example:** • **500 GB for document storage** • **100 GB for database storage**	Dedicated storage space: Click here to enter text.

8. Have you obtained required trusted-signed certificates?	Yes ☐ No ☐
9. Have you obtained the required Microsoft license keys? (Windows Server 2016 and Office 2016 Standard or Professional edition)	Yes ☐ No ☐

Firewall Connectivity Matrix

The firewall connectivity matrix details the access settings required for the BlackBerry Workspaces product. These settings must be configured by the customer to enable BlackBerry Workspaces service.

Note: end-users accessing BlackBerry Workspaces require access only to the "Main" server over HTTPS protocol.

Appliance-X Basic

Source	Target	Port
Main RHEL Server	SMTP Server	• 25
Main RHEL Server	Conversion Windows Server	• 22 • 4510 • 4511 • 5666 • 443 • 4431 • 4432 • 4433 • 8082
Conversion Windows Server	Main RHEL Server	• 4510 • 4511 • 8543 • 8443 • 53 (+UDP) • 4505 • 4506
End User Devices	Main RHEL Server	• 80 • 443
IT Admins	Main RHEL Server	• 5000 • 8081

BLACKBERRY

Appliance-X Advanced

Source	Target	Ports
Orchestration server	SMTP server	• 25
Orchestration server	Main server	• 22 • 5666
Orchestration server	Frontend server	• 22 • 5666
Orchestration server	Application server	• 22 • 5666
Orchestration server	Conversion-Windows server	• 22 • 5666 • 4510 • 4511
Main server	External Cloud Storage	• 443
Main server	Orchestration server	• 4505 • 4506 • 8543
Main server	Frontend server	• 3000
Main server	Application server	• 8009 • 8080
Main server	Conversion-Windows server	• 443 • 4431 • 4432 • 8082
Main server	Main server	• 6379
Frontend server	Orchestration server	• 4505 • 4506 • 8543
Frontend server	Application server	• 8009 • 8080
Frontend server	Main server	• 53 (+UDP) • 8443
Frontend server	Conversion-Windows server	• 443 • 4433
Application server	SMTP server	• 25
Application server	Orchestration server	• 4505 • 4506 • 8543
Application server	Main server	• 3306 • 8443 • 8081 • 11211 • 2049 • 111

		• 53 (+UDP)
Application server	Frontend server	• 3000
Conversion-Windows server	Orchestration server	• 4505 • 4506 • 8543
Conversion-Windows server	Main server	• 8080 • 8443 • 53 (+UDP)
End User Devices	Frontend server	• 443 • 80
IT Admins	Orchestration server	• 5000 • 7767
IT Admins	Main server	• 8081

Disaster Recovery

If Disaster Recover (DR) is used, the following ports should also be opened.

Source IP	Target IP	Port Number	TCP/UDP
Orchestration (Primary)	Orchestration (Secondary)	22	TCP
Orchestration (Primary)	Main (Secondary)	22 3306	TCP
Main (Primary)	Orchestration (Secondary)	22	TCP
Main (Primary)	Main (Secondary)	22 111 1039 1047 1048 2049 3306	TCP TCP & UDP TCP & UDP TCP & UDP TCP & UDP TCP & UDP TCP
Orchestration (Secondary)	Orchestration (Primary)	22	TCP
Orchestration (Secondary)	Main (Primary)	22 3306	TCP
Main (Secondary)	Orchestration (Primary)	22	TCP
Main (Secondary)	Main (Primary)	22 111 1039 1047 1048 2049 3306	TCP TCP & UDP TCP & UDP TCP & UDP TCP & UDP TCP & UDP TCP
Orchestration (Primary)	Frontend (Secondary)	80	TCP
Main (Primary)	Frontend (Secondary)	80	TCP

Orchestration (Secondary)	Frontend (Primary)	80	TCP
Main (Secondary)	Frontend (Primary)	80	TCP

BLACKBERRY

Hardware Requirements

The hardware specifications can be found below. Please reference the server sizes based on the below Server Sizes chart.

Server Sizes

Server size	Local operating system storage	Memory	Processors (CPU/vCPU)
Small	100 GB	10 GB	2
Medium	100 GB	10 GB	4
Large	100 GB	12 GB	6
X-Large	100 GB	16 GB	8

Appliance-X Basic

Server name	Server size
Master-Main	X-Large
Conversion - Windows	Medium

Appliance-X Advanced

Server name	Server size	Comments
Orchestration	Small	-
Frontend	Small	Depending on enterprise scale requirements, a larger server size might be recommended.
Main	Large	Depending on enterprise scale requirements, a larger server size might be recommended.
Application	Medium	-
Conversion - Windows	Medium	-

Additional File Storage

In addition to the OS drives, 3 additional disks are required to store end users' uploaded files and database files. Data stored on these drives will remain encrypted at all times. Depending on the deployment option selected, the drive mount points will differ.

Deployment Type	Disk Purpose	Server Location	Mount Point	Size
Basic AppX	Filespace	Master-Main	/opt/watchdox/storage/filespace	Customer Discretion
	Database	Master-Main	/mnt/database	20% of Filespace
	FS Cache	Master-Main	/opt/watchdox/storage/fs_cache	25 GB
Advanced AppX	Filespace	Main	/opt/watchdox/storage/filespace	Customer Discretion
	Database	Main	/mnt/database	20% of Filespace
	FS Cache	Main	/opt/watchdox/storage/fs_cache	25 GB

Server Images

BlackBerry can supply non-licensed versions of both Red Hat Enterprise Linux and/or Windows Server 2012 R2 to be used with the deployment, which can be found here:
<https://watchdox.watchdox.com/ngdox/workspaces/303688/>

If the customer chooses to use their own images for deployment, please adhere to the following requirements:

Servers	Requirements
Red Hat Linux Enterprise	- Static IP for each server - Red Hat 6.4 – Red Hat 6.8. RHEL version. 7.X+ is not yet supported - Root account or a personal user account with full SUDO permission (with NOPASSWD). The BlackBerry Workspaces operations team uses this account to log in to machines for maintenance. - SSH service is available and running - SELinux is either disabled or in permissive mode - eth0 Ethernet interface is enabled
Windows	- Static IP for each server - Windows Server 2016 64-bit is activated - Microsoft Office 2016 64-bit, Standard or Professional is activated - Validate that the C: and D: drives were created (100 GB each) - Create the D:\Temp directory with FULL permission assigned to all users - Set environment variables %TEMP% and %TMP% for system, user, and default user to D:\Temp - Choose: - To use SSH: Ensure the BlackBerry Workspaces Cygwin package is installed. The installer is provided before deployment and includes these packages: - openssh

	o vim
	o zip
	o unzip
	o wget
	o rsync
	o curl
	o cygrunsry
	o dos2unix
	o python 2.6
	• To use SMB:
	    o Run the "command Set-ExecutionPolicy unrestricted"
	      Powershell command before deployment

Additional Connector Add-Ons

BlackBerry Workspaces supports Connectors that allow the organization to utilize other third-party services to incorporate with Workspaces. The Connectors include services such as SharePoint, Windows File Share, and Single Sign On services via SAML. The following are prerequisites that should be completed prior to installing the Connectors:

UCC (Unified Content Connector)

If the customer will be installing the UCC to support integration with SharePoint on-prem, SharePoint Online, Windows File Share, or One Drive for Business, then an additional Windows server will be required. Below you will find the prerequisites for this Connector:

Server Size

- OS: Windows Server 2016
- CPU: 4 vCPU
- Memory: 8 GB
- Storage: 100 GB

Port Requirements

Source	Target	Port
Master-Main server (Basic deployment) **or** **Main server (Advanced deployment)**	Unified Content Connector	8443
Unified Content Connector	External Repository	Per third-party service requirements (usually 443)
Unified Content Connector	Frontend server (Advanced deployment)	443

Single Sign-On Identity Connector

No additional server is required for Single Sign-on via SAML. The customer is expected to already have a single sign-on service in place prior to the configuration. If you need recommendations for a third-party SAML provider, please contact your BlackBerry Professional Services Consultant, and they can assist.

Email Protector

The Email Protector requires at least one additional RHEL server. Please see the below prerequisites for this Connector:

Server Size

- OS: Red Hat Enterprise Linux 6.X
- CPU: 4 vCPU
- Memory: 8 GB
- Storage: 100 GB

Port Requirements

Source	Target	Port
Master-Main server (Basic deployment) **or** **Frontend server (Advanced deployment)**	Email Protector	• 25 TCP • 443 TCP
External Mail server	Master-Main server (Basic deployment) Or Workspaces Frontend server (Advanced deployment)	• 8891 TCP
Workspaces	Frontend server (Advanced deployment)	• 443 TCP

Office Online Server

The customer is expected to already have installed a working version of Office Online Server (OOS) or Office Web Apps Server (OWAS). There is no additional server required to connect Workspaces with an existing Office Online environment.

Port Requirements

Source	Target	Port
Master-Main server (Basic deployment and vApp) **or** **Application server (Advanced deployment)**	OWAS or OOS	443 (HTTPS)
OWAS **or** **OOS**	Master-Main server (Basic deployment and vApp) or Application server (Advanced deployment)	443 (HTTPS)

End-user machine	OWAS or OOS	443 (HTTPS)
OWAS **or** **OOS**	End-user machine	443 (HTTPS)

BLACKBERRY

Appendix

SSL Certificates

The BlackBerry Workspaces Virtual Appliance must be provisioned with SSL certificates by an approved certificate authority. The SSL certificate should be generated before the installation. There are many ways to generate a CSR (Certificate Signing Request). BlackBerry recommends the following, which can be performed on almost any Linux server from the Terminal. Once complete, submit the CSR to your Certificate Authority and retain the Private Key:

```
openssl req -new -newkey rsa:2048 -nodes -keyout /tmp/privateKey.key -out
/tmp/CSR.csr
```

The Appliance-X installation requires 3 certificate pieces:

- **SSL Certificate**

  o Definition: The SSL certificate that will be used to secure communication with end users. This certificate should have the site's URL in either the Subject Name or Subject Alternative Name (SAN) attributes. This must be signed by a valid 3rd party, publicly trusted certificate authority (not self-signed or internally signed).

  o Sample:

    -----BEGIN CERTIFICATE-----

    MII/………

    ……………………

    -----END CERTIFICATE-----

  o Further information: http://technet.microsoft.com/en-us/library/cc778623(v=ws.10).aspx

- **SSL Certificate Private Key**

  o Definition: This is the private key used to decrypt the communication.

  o Sample:

    -----BEGIN PRIVATE KEY

    ….

     -----END PRIVATE KEY-----

o Further information: http://www.tldp.org/HOWTO/SSL-Certificates-HOWTO/x64.html

- **SSL Intermediate CA Bundle**

    o Definition – a combination of the certificates validating the SSL site certificate. This bundle usually contains 2-3 certificates, including the intermediate and root certificates.

    o Sample:

    -----BEGIN CERTIFICATE-----

    MIIE5T…

    -----END CERTIFICATE-----

    -----BEGIN CERTIFICATE-----

    MerR….

    -----END CERTIFICATE-----

    o Link: http://en.wikipedia.org/wiki/Intermediate_certificate_authorities