

# Syncplicity IT Readiness Guide

How a customer prepares their environment to deploy Syncplicity

## **Abstract**

This white paper explains the necessary prerequisites to be completed prior to deploying Syncplicity either in the cloud or on-premise.

Published July 2013

Copyright © 2013 EMC Corporation. All Rights Reserved.

EMC believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

The information in this publication is provided “as is.” EMC Corporation makes no representations or warranties of any kind with respect to the information in this publication, and specifically disclaims implied warranties of merchantability or fitness for a particular purpose.

Use, copying, and distribution of any EMC software described in this publication requires an applicable software license.

For the most up-to-date listing of EMC product names, see EMC Corporation Trademarks on [EMC.com](http://EMC.com).

**Table of Contents**

- CONFIGURING VPN SERVERS FOR SYNCPLICITY .....4**
  - For Mobile Users..... 4
  - Core to communication from both the clients to the SaaS stack. .... 4
  - Used to pull client data and roll up to the admin portal. .... 4
  - API’s used for the online file browser ..... 4
  - Instrumentation that serves monitoring & metering capability for t he client to the service to monitor uptime. .... 4
  - Gravatar service..... 4
  - Online file browser – presentation..... 5
  - Elements in the “Show detailed status” page / popup in the desktop client ..... 5
  - Manuals ..... 5
- CONFIGURING PROXY SERVERS FOR SYNCPLICITY .....5**
- CONFIGURING EMAIL SERVERS FOR SYNCPLICITY .....5**
- CONFIGURING FOR ON-PREMISE STORAGE .....5**
  - Prerequisites for Syncplicity Storage Connector (Compute Nodes) ..... 6
  - Load Balancing Options..... 6
- Additional Resources .....7**

## **CONFIGURING VPN SERVERS FOR SYNCPLICITY**

Syncplicity uses HTTPS on port 443 (needs to be open system-wide) and a series of URLs need to be whitelisted on the firewall to ensure that all the users have a seamless experience when they start installing and using the Syncplicity client on their PC and/or Mac devices and logged into the corporate network or using VPN for remote connections to the corporate networks:

### **For Mobile Users**

- m.syncplicity.com:443
- ml.syncplicity.com:443

### **Core to communication from both the clients to the SaaS stack.**

ds.xx should be whitelisted for a cloud storage deployment, but can be blocked for on-premise storage. For on-premise storage the data path would route traffic to the respective on-premise storage system.

- My.syncplicity.com:443
- Datastore.syncplicity.com:443
- Ds-xx.syncplicity.com:443 (where xx can be 00 to 99)
- Download.syncplicity.com:443
- Ds-bart.syncplicity.com:443
- Manual.syncplicity.com:443
- xml.syncplicity.com:443

### **Used to pull client data and roll up to the admin portal.**

- SSL.google-analytics.com:443

### **API's used for the online file browser**

- Fonts.googleapis.com:443

### **Instrumentation that serves monitoring & metering capability for the client to the service to monitor uptime.**

- Beacon-1.newrelic.com:443
- Lfov.net:443

### **Gravatar service**

Part of the news feed / rss feed and serves thumbnails. Disabling it would simply show a grey avatar box in the news feed

- Secure.gravatar.com:443

## Online file browser – presentation

- Ajax.aspnetcdn.com:443
- Ajax.googleapis.com:443

## Elements in the “Show detailed status” page / popup in the desktop client

- Pixel.quantserver.com:443.

## Manuals

- PBworks is an online web-based publication tool used for manual.syncplidity.com
- Files.pbworks.com:443

## CONFIGURING PROXY SERVERS FOR SYNCPLICITY

If using a Proxy Server routing of xml.syncplidity.com:443 is enabled

## CONFIGURING EMAIL SERVERS FOR SYNCPLICITY

Whitelist ‘Syncplidity.com’ domain on all email servers

Ensure that there is no limit on file size download on the network as this deprecates the user experience when trying to sync large files.

## CONFIGURING FOR ON-PREMISE STORAGE

The Syncplidity Storage Connector is delivered as a virtual machine image (in an OVA format) to greatly simplify the deployment process. The virtual machine image is based on the CentOS 6.4 Linux distribution, and ships with the necessary Syncplidity software, and its dependencies, pre-installed.

Technical Overview and deployment of an Enterprise Edition Installation

<http://manual.syncplidity.com/w/page/64354670/Enterprise%20Edition%20Features>

Install guide for On-premise Storage <http://manual.syncplidity.com/w/page/64578429/On-Premise%20Storage%20Installation%20Guide>

Virtual Machine Provisioning -- Begin the process by downloading the Syncplidity Storage Connector OVA file from <http://download.syncplidity.com/storage-connector/SyncplidityStorageConnector.ova>

Once downloaded, connect to the appropriate VMware ESXi server using VMware vSphere Client and perform the following steps once for each compute server you will be deploying (at least twice)

On-premise storage settings <http://manual.syncplidity.com/w/page/64577465/On-Premise%20Storage%20Settings>

## Prerequisites for Syncplicity Storage Connector (Compute Nodes)

### Hardware requirements

- A minimum of two virtual machines hosted on VMware vSphere Hypervisor (i.e. ESXi) 5.0 and 5.1
- Each virtual machine is configured with 8GB of RAM, 8 virtual cores (Intel Xeon E5 Family processors, 2.20 GHz), and a 25GB HDD
- (OPTIONAL) An externally addressable SSL-offloading Load Balancer in front of all virtual machines, configured with a CA-signed (NOT self-signed) SSL certificate
- A supported storage backend File System via NFS 3.0 (ISILON, VNX); Object Storage APIs (ATMOS, VIPR) and S3 APIs (AMAZON S3, EMC VIPR)

### Open Ports

The compute application has the following open port requirements:

INBOUND port 443 FROM anywhere -- only if node exposed directly to Internet

INBOUND port 443 FROM load balancer -- only if node behind a non-SSL offloading loads balancer

INBOUND port 80 FROM load balance -- only if node behind an SSL offloading loads balancer

INBOUND port 22 FROM trusted hosts on internal network that manage the node

OUTBOUND port 443 TO xml.syncplicity.com

OUTBOUND port 80 TO download.syncplicity.com

OUTBOUND port 443 TO Atmos load balance - only with Atmos, only if HTTPS is used

OUTBOUND port 80 TO Atmos load balancer - only with Atmos, only if HTTP is used

### Load Balancing Options

With a set of compute application instances deployed inside the enterprise data center, file transfer traffic from Syncplicity clients must be evenly distributed to ensure proper utilization of available resources. Here are three common load balancing options:

#### On-Premise Load Balancing

An administrator provisions one or more compute application instances and places them all behind a hardware or software load balancer. The load balancer's IP address is registered with a singular DNS hostname, and the hostname is registered with the company's Enterprise Edition account. All traffic flows through the load balancer. The load balancer is in charge of distributing traffic evenly across the set of available instances, ceasing to forward traffic to downed instances, and beginning to flow traffic to newly created instances. The unique upside with this option is the lack of reliance on any external factor or mechanism for load balancing. The load balancing process is invisible to Syncplicity clients, Syncplicity orchestration, and the DNS server. The internal load balancer can react immediately to up/down state changes of the backend instances. Nevertheless, this option requires the most work and expense on the part of the network administrator.

## DNS Round-Robin Load Balancing

An administrator provisions one or more compute application instances and configures a DNS record for the same hostname that resolves to a list of IP addresses for all the provisioned instances. The administrator subsequently registers the singular hostname with the Enterprise Edition account. When Syncplidity clients perform a DNS resolution against the singular hostname, the DNS server will return one of the IP addresses in its list in a round-robin manner, assuring proper distribution of load. As instances are added to or removed from the on-premise deployment, the DNS record must be kept up to date. Administrators must keep in mind DNS caching performed by intermediate DNS servers and ensure that the DNS refresh interval is set appropriately.

## Syncplidity-Driven Application-Level Load Balancing

An administrator provisions one or more compute application instances, assigns a unique hostname to each one, and registers all hostnames with the Enterprise Edition account. The administrator may use the administration console or the Syncplidity API to register and deregister hostnames. Syncplidity subsequently distributes a random hostname to each connected Syncplidity client. Whenever a client is unable to reach a compute application instance behind a specific hostname, the client will re-query the orchestration component for a new one. This ensures that a client always has a working compute application instance to work with. When Syncplidity is in charge of load balancing across the enterprise compute application instances, the list of hostnames available to it must always be up to date. This means that manual or automated (via the Syncplidity API) intervention is required anytime instances are added or removed from the on-premise deployment.

## Additional Resources

- [Syncplidity Enterprise Edition Online Manual](#)
- [Syncplidity Technical White Paper: EMC Isilon](#)
- [Syncplidity Technical White Paper: EMC Atmos](#)
- [Syncplidity Technical White Paper: EMC VNX](#)
- [Getting Started with Syncplidity and Active Directory](#)