# Pre-deployment Checklist

SUPPORT

□ Gigabit connections from the Datto to all relevant network infrastructure (Check switch ports, try to have the Datto appliance on a gigabit switch whenever possible)

□ Firewall rules:

**a.** From protected machine to Datto appliance: UDP 139 and TCP 25566 (Live when the StorageCraft Raw Agent service is enabled and running)

**b.** From Datto appliance to internet: 22, 80, 123, 443 outbound to at minimum the following addresses:

**i.** 8.25.163.66: update.dattobackup.com, checkin.dattobackup.com device.dattobackup.com

**ii.** 209.118.59.2: update.dattobackup.com, checkin.dattobackup.com, device.dattobackup.com

**iii.** 8.25.163.80: heartbeat.dattobackup.com

**iv.** 209.118.59.244: packages.dattobackup.com

**v.** 209.118.59.250: mirror.dattobackup.com

□ Remove all other backup software present on the system to be protected. When removing, try to use a high level uninstaller that removes all traces of the program after deployment, including registry keys, dlls and stray folders.  These may represent components that still threaten to produce conflicting scenarios. Reboot server once all other backup software has been removed.

□ Server state is important before deploying a backup agent:

**a.** Hardware health: All RAIDs report back as healthy, individual disks report back as healthy via chkdsk. Disk repairs should immediately be remedied before the deployment of any backup agent. Failure to do so may result in backing up corrupted systems.

**b.** Event Viewer: Check the targets system and application logs to see if there are any VSS or hardware errors that appear. Resolve any errors found on the server before attempting to install the agent.

**c.** Given the server's application, additional considerations may need to be accounted for:

**i** SQL: Check for SQL backups that may be taking place. If you want to account for these backups as well, make sure they are on a partition being backed up. Do note that your backups will be larger if you choose to perform these steps.

# Pre-deployment Checklist

ii Exchange: We recommend that circular logging be disabled when utilizing our backup agent. VSS backups will truncate logs upon completion. Make sure that the Exchange writers are enabled per your operating system. Also, check for additional archiving tools such as auto-archiving that may cause larger incremental changes.

iii. DFS: Distributed file systems on servers that stage and replicate files and folders to other places may also account for larger backups. Consider the role of DFS before deployment and consider that it may take larger backups if the files are staged at a particular time. DFS by default shouldn’t cause large changes as long as the transfers are occurring as expected and VSS writer that maintains them remains stable.

iv. Hypervisors: We recommend that hypervisors have their datastores isolated on a separate partition, and that the non-datastore volumes be backed up by the ShadowSnap agent. Servers that may reside on the datastore should be backed up individually to allow for more granular recovery and restore efforts.

v. Clustering: ShadowSnap does not officially support backing up high-availability clusters due to the way that the disks are created and maintained within the clusters.

vi. Proxies: ShadowSnap and ShadowProtect do not support the use of proxy servers on the network. Agents are required to check in to StorageCraft to verify their license monthly

d. Disk defragmentation: While we can support backups that are running disk defragmentation, do be aware that this rearranges data at a block level, and larger backups will consequently result. Run a disk defragmentation before deployment of the agent. VSS-aware disk defragmentation programs may allow for smaller backups, but this would be left to your own discretion.

❑ Latest installer for the ShadowSnap agent can always be found here: www.shadowsnap.com

❑ Reboot Server