SUPPORT

Preparing for a ShadowSnap Deployment

Network Requirements

Local Area Network Connection

Gigabit connections are required between all protected machines on the network. This also means that the Datto should be at the physical site as all the protected machines, otherwise there will be a need to unnecessarily extra variables for local backups and disaster recoveries.

Note: Keep in mind the initial data that will transfer across the network can span from hundreds of gigabytes to terabytes in size. Without any other traffic on the network, 100Mbps networks are capable of transferring up to 45GB per hour. Therefore a 100Mbps network is incapable for providing a reliable & efficient backup & disaster recovery solution.

ShadowSnap Agent Installation

TCP Ports 139(SMB) and 25566(ShadowSnap) must be open between the Datto and all protected machines. If these ports are blocked or filtered, the ShadowSnap Agent Service will not be able to communicate with the Datto device.

FOR ENCRYPTED AGENTS: To have successful production machine backups with encrypted agents Port 3260 needs to be open bi-directionally between the Datto and the Production Machine. This port allows iSCSI to transfer encrypted data through SAMBA.

Protection of a Server in a remote location over a WAN

50Mbit dedicated uplink from the ShadowSnap Agent to the Datto for every Terabyte of protected data set size is required for reliable backups to be performed.

Example: A 2TB protected machine that is located at a remote location will require a 100Mbit uplink from that remote network back to the Datto device.

The Datto Siris ShadowSnap solution has two components, ShadowSnap and ShadowProtect. Both of these components are required to operate the agent with the Datto web interface. The ShadowSnap interface is non-existent on the locally protected machine; however an interface for ShadowProtect is available from the Start menu of a protected system with the full ShadowSnap package installed. Both components should be verifiable as installed in Add/Remove Programs.

ShadowProtect - Backup Software

ShadowProtect acts as a VSS requester, allowing the full set of VSS writers installed on the protected system to act as its primary backup engine and deliver Application-aware backup images. In case of failures in specific VSS providers, ShadowProtect also has a fallback StorageCraft Shadow Copy Provider, that places requests only to the most central VSS writers to deliver a crash-consistent state backup.

ShadowSnap - Remote Agent

ShadowProtect as managed by the ShadowSnap remote agent is a volume based backup solution, which means that it backs up entire partitions, not individual files and folders. In preparation for deployment, if there is data that does not need to be imaged, it needs to be relocated to a separate partition which can then be excluded from images.

As the ShadowSnap solution is a volume based backup provider, any block level change on the protected agent will be accounted for in backup. This includes other backups, certain maintenance tasks, or failures that interfere with the file system. ShadowSnap can only back up volumes that are recognized by the Windows operating system as local, stable volumes.

For more information on distinctions between ShadowProtect Backup Software and ShadowSnap Remote Agent see ShadowProtect and ShadowSnap

Considerations for Deployment:

- Backup software is like antivirus software, having more than one in place is often problematic as they may encounter a conflicting scenario. Problems may not arise immediately if the solutions do not encounter an error right away. Disable or ideally 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.

- Acronis will typically prevent installation of the ShadowSnap agent. However, for any previous Acronis deployment, check out this tool for removing that software in its entirety: Removing Acronis

- Server state is important before deploying a backup agent:

- Windows updates, service packs, and any other Microsoft provided updates should be downloaded to the target machine and the appropriate reboots to be taken place (Remember that the 2nd Tuesday of every month is patch Tuesday for Microsoft, consider this for deployment windows)

- **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 and can result is restoration failures.

- **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.

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

SQL: Check for SQL maintenance jobs that may be taking place, they are in effect a separate backup solution. Datto recommends to have SQL maintenance jobs saved to a partition that is unprotected by the Datto, so local backups are not extraordinarily large. If the Datto is set to protect the volume that has the SQL maintenance jobs saved then the local Datto can fill up and the device could potentially not sync offsite properly. Best Practices for SQL servers can be found here.

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.

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.

Hypervisors: Datto 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. Best practices for backing up hypervisors can be found here.

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.

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.

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.

StorageCraft Preinstall Check

One great place to start before a ShadowSnap deployment is here: StorageCraft Preinstall Check

This is a pre-install checker for the ShadowProtect software platform. While not directly related to ShadowSnap, it will ensure optimal installation of the ShadowProtect software which ShadowSnap interacts with. There are several considerations brought forth by this pre-install checker and are all reviewed on StorageCraft's website and knowledge base. While not 100% necessary, the check is quick and can provide insight on how to improve your server's backup reliability and performance down the road.

Server Tuning

Here is another excellent resource from Datto's partners at StorageCraft: StorageCraft Server Tuning Guide

Many of these settings can significantly improve the reliability of the backups, especially any network latency issues or disk input / output issues. Since some of these steps involve manipulating the registry, take a backup of the registry before making any changes.

Pre-deployment checklist

❑ 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

Note: These ports are responsible for providing communication between the Datto devices and Datto's Remote Monitoring Servers. Features which use these ports include: Remote Web, Remote VNC, Cloud Sync, Datto OS Auto-Updates, reporting & alerting.Datto's main backup engine is ShadowSnap, currently in version 3.0.24225

After the server has been checked, you can run the installer. While you can schedule a reboot later, you will need to reboot before the backup driver can be loaded. At this time, you may pair the agent to the Datto device and begin configurations. However, a backup will not be able to run until after the reboot.

Verify Installation

- Make sure that all 3 essential services are present and running:
    - ShadowProtect Service
    - StorageCraft Raw Agent
    - StorageCraft Shadow Copy Provider (Windows 2000 Machines will not have this present, Windows 2000 pre-dates Shadow Copies)
    - A Quick test of the services would be to restart from services.msc and see if they stop and start cleanly.
    - Open up the ShadowProtect software on the device. The lower left tab should show an active license.
    - Check out the agents tab, the agent should populate as ready to accept a backup.

Best practices for setting up schedules and initial configurations:

- Consider your client's need and discuss this with them before providing the schedule: how far would you need to feasibly go back to retrieve data? Set the expectations with them and provide a schedule accordingly. Set the local data retention policies based on these conversations and expectations. Remember that long-running retention policies will require more disk space, and should be considered when sizing an appliance.
- Consider the server's application: while a file server may need to be backed up during business hours as files are in constant change, a terminal server that simply houses configurations may not require as many backups per day as there is little to no change provided. Backups are just like any other service on a server, they consume resources and take disk input / output. Consider this while setting a schedule.
- Before you take the first backup, make sure that any volumes that you do not want to be backed up are excluded from the advanced options tab. Remember that any additional drive that is attached to the machine may attempt to be backed up (USB drive, additional storage drive, etc.)

For information on other Datto Siris configurations, see also Configuring Portal Alerts and AgentSync

ShadowSnap Minimum System Requirements

Windows 2000
Windows XP
Windows Server 2003
Windows Vista
Windows Server 2008
Windows 7
Windows 8
Windows Server 2012 without Deduplication turned on

Note: Scope of support for these Operating Systems covers all variants such as either 32bit or 64bit versions.

Supported Disk Volume Types

- Basic and Dynamic Disks
- NTFS
- Hardware and Software based arrays
- Any sized disk, including disks larger than 2TB in size.
- GPT / MBR

Windows Guest Operating Systems that are supported under Supported Operating Systems with native hypervisor disk formats of:

- VHD
- VMDK
- VDI
- QCOW

Available Space Of Each Protected Volume

- Windows 2000: 500MB
- Windows XP & 2003: 1GB
- Vista, 2008, & Newer: 2GB

Web Browser

All Datto Web Interfaces are developed for use with the Mozilla Firefox browser.

Other browsers such as Internet Explorer, Chrome, & Safari will function most of the time, but for the best experience please use Mozilla Firefox.

Datto Inc.
101 Merritt 7
Norwalk, CT 06851
www.dattobackup.com

USA: 888.294.6312
Canada: 877.811.0577
UK: (01224) 451475