Backup

While the Skytap platform has a point in time cloning system, using the [Template an Environment feature](https://help.skytap.com/saving-an-environment-as-a-template.html), this is not designed to replace a comprehensive backup strategy. It is not a replacement for live systems such as online Databases or Application servers.

Most organisations will already have a defined backup strategy and preferred vendors, assuming these vendors do not require a physical appliance to be installed into Skytap they should be compatible with the platform.

##### Supported Implementations

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Application | Vendor | x86 | | Power | | | Reference Architecture |
| Windows | Linux | AIX | IBM i | Linux |
|  | Veeam | ✔️ |  | ✔️ |  |  |  |
|  | Storix |  |  | ✔️ |  |  | ✔️ |
| BRMS | IBM |  |  |  | ✔️ |  | ✔️ |
| Commvault | Commvault | ✔️ | ✔️ | ✔️ | ✔️ | ✔ | ✔️ |

#### Secrets Management

The Skytap platform utilizes at rest encryption on all storage and strong in transit controls through our portal or API. However, these aren’t designed to protect application secrets that may become compromised due to development errors; application or operating system vulnerabilities; or bad actors. To secure application secrets, license keys, and sensitive customer information a secrets manager can provide controlled access and encryption services for these functions.

##### Supported Implementations

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Application | Vendor | x86 | | Power | | | Reference Architecture |
| Windows | Linux | AIX | IBM i | Linux |
| [Vault](https://www.vaultproject.io/) | HashiCorp | ✔️ | ✔️ | ✔️ | ✔️ | ✔️ |  |
|  |  |  |  |  |  |  |  |

#### Log Management

Most organisations will have already deployed an on-premises, or in cloud, log management tool to either deliver Security Incident Event Management (SIEM), operations management or both. Application and Operating Systems logs should be funneled into this system to provide both Security and Operations teams a holistic view of their estates.

To simplify management and security, consolidating these logs into a single sender per environment or per customer account is preferred. All Virtual Machines and LPARs should send logging traffic to this sender for onwards propagation to the log management solution.

##### Supported Implementations

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Application | Vendor | x86 | | Power | | | Reference Architecture |
| Windows | Linux | AIX | IBM i | Linux |
| [Splunk Cloud](https://www.splunk.com/en_us/software/splunk-cloud.html) [Splunk Enterprise](https://www.splunk.com/en_us/software/splunk-enterprise.html) | Splunk | ✔️ | ✔️ |  |  |  |  |
| syslog | | ✔️ | ✔️ | ✔️ | ✔️ | ✔️ |  |