ZYNSTRA TECHNICAL BRIEFING NOTE

Patching and Release Schedule

Introduction

Each Zynstra appliance comprises a software platform created by Zynstra and a server hardware platform supplied by Hewlett Packard. The appliances are the foundation of a managed service whose scope is consistent across all customers, a service that includes the on-going maintenance and enhancement of the software platform during its life on the customer's premises. Maintenance and enhancement is achieved through the following controlled changes to the appliance:

- **Software releases**

  These are software releases made by Zynstra that introduce new capabilities to extend the software's functional capabilities, enhance its manageability, improve its performance and much more besides. They also address defects and vulnerabilities that are not believed by the relevant software vendor to be either critical or important.

- **Important software patches and security updates**

  The patches address software platform defects where the vendor of the affected software believes that those defects to be 'critical' or 'important' because they could create (or could imminently create) serious issues with respect to the availability of the software platform for its intended use or risk of loss of or damage to the integrity of the customer's data. The updates are enhancements to the security software on the appliance to address threats identified by the vendor of that software which are deemed to create an immediate or short-term risk to the availability of the software platform for its intended use or to the privacy or availability of the customer's data.

- **Urgent software patches and security updates**

  These software patches and security updates are few and far between and comprise the most urgent of the critical software patches and security updates issued by software vendors. A patch or update is deemed by Zynstra to be urgent if, in Zynstra's sole opinion, it believes that the defect or vulnerability will have an immediate and catastrophic effect on the appliance and/or the privacy or integrity of the customer's data. Such patches and updates are ones which Zynstra believes cannot wait until the next occasion on which critical and important software patches and updates and software releases are to be applied.

Service Continuity Impact of Patches, Updates and Releases

The above patches, updates and releases will result in some partial (or even complete) loss of service on the appliance during their application. For patches and updates, this loss of service is generally only a matter of a few minutes and there may only be a partial loss of service anyway. For software releases, the loss can in certain cases last many hours and will often result in a complete loss of service.

Other than these patches, updates and releases, the only activity performed on each appliance that is expected to cause a partial loss of service is the creation of snapshots of software images prior to them being backed up, both locally and to the Cloud. All the software images on each appliance are backed up in full once each week and the Active Directory image (including the AD user data) is backed up incrementally each night as well. This activity commences at or later than 2300 in the time one in which the appliance is located. As each image is snapshotted to create a backup copy, it becomes unavailable for use for just a few minutes and is then restored again immediately.

Patching and Release Schedule

Fundamental to the effectiveness and cost-efficiency of the managed service is the requirement for all customers to use the very latest version of the software platform, with only minor deviations from this principle being permitted in order to address customer-specific timing issues (such as a critical business deadline). Customers therefore cannot 'opt-out' entirely from any individual patch, update or release – they can simply request minor adjustments to the date of its application.

Zynstra works to a pre-determined schedule when applying important software patches, security updates and software releases. This means that customers know in advance exactly when changes will be made to their appliance and they can (a) plan for the service loss that may occur, or (b) notify Zynstra on a case-by-case basis of any important business reasons why the patch, update or release needs to be moved to a different time. Any change to the schedule is always subject to the customer's acceptance of responsibility for the resulting interim risks to the reliability of the appliance and the availability, privacy and integrity of their data.

The sole exception to the pre-determined schedule is for the application of any urgent software patches and security updates which need to be applied as soon as possible after they have been tested/validated by Zynstra.

The application of critical and important software patches and security updates as well as software releases to an appliance takes place during one of four patching timeslots each calendar month. Each customer is allocated a default timeslot when they place an order based on the first letter of the name by which they are known to Zynstra:

First Letter	Default Timeslot	Patching Date and Time in Month
A – F	T1	First Thursday night
G – L	T2	Second Wednesday night
M - R	T3	Third Tuesday night
R – Z	T4	Fourth Monday night

The above timeslots all start at 2100 in the time zone in which the appliance is located.

For example, a customer called Aardvark would receive patches and releases during a timeslot starting at 2100 on the first Thursday in each month.

A new customer can move to a different timeslot (Tx) by requesting a change through the support service for their appliance. If a customer wishes to move to a different timeslot for one month only, perhaps due to important business commitments which mean that they do not wish any changes to be made to their appliance during their usual timeslot, they can do so again through the support service for their appliance.

Zynstra may ask a customer to move to a different patching and/or release timeslot from their default (or to spread their appliances across multiple timeslots in the case of very large multi-site customers).

For operational reasons, Zynstra may also ask a customer if it is possible to apply a patch, update or release outside their normal timeslot, giving at least two working days notice of its desire to do so. Customers may refuse the request if it is inconvenient in which case the work would be performed during the pre-agreed timeslot.

Urgent software patches and security updates are generally applied to every appliance as soon as the patch or update becomes available. Zynstra provides notification of its intention to do so by 1200 on the day on which the urgent patch or update is to be applied overnight. Provided that Zynstra receives a request to postpone by 1800 the same day, it will postpone the patch or update for a short period provided that the customer fully accepts the risks associated with postponement.

After the application of any patch, update or new release, notification will be provided within four working hours if and only if the application failed for any reason and it needs to be repeated. It should be noted that any such failure will not adversely affect the functioning of the appliance as changes are automatically reversed in the event of any failure during or at the end of the application process.