



System State Protection

CA ARCserve® Replication and CA ARCserve® High Availability (formally known as CA XOssoft™ Replication and CA XOssoft™ High Availability) provides continuous data protection and high availability for Windows, Linux and UNIX® environments on physical and virtual servers. System State Protection provides automatic disaster recovery protection through multiple point-in-time copies of the local system state that are then replicated and stored on the Replica server. It lets you create a backup file for critical system related components and recover the data after a system failure. Apart from protecting your mission critical applications and data, it is equally important to protect the operating system files. System State data is a crucial component that needs to be backed up to keep your systems running; losing important system files implies the system cannot be booted or run properly. Without a stable Operating System environment, applications cannot provide stable services.

OVERVIEW

System State Protection allows you to include critical system-related components in your replication and high availability scenarios, enabling you to recover these components in the event of a system failure.

System State Protection lets you protect the system state including registry hive files, COM+ database, and boot files. You can specify periodic backup intervals, send the snapshot file to more than one replica server and restore data from a System State snapshot.

BENEFITS

- Enables you to configure System State Protection in the Scenario Creation Wizard
- Set up periodical schedule to automate system state protection.
- Protects performance counter configuration, Active Directory, SysVol folder, Certificate Server, Cluster Database, Registry, and COM+ Database depending on the OS.

Install/Configure

Installation of CA ARCserve Replication and High Availability is straightforward and wizard driven. The Installation does not require any reboot or application shutdown. You need to install CA ARCserve Replication or High Availability Engine on both the Master and Replica servers. You do not need any additional license to protect your system state using the System State Protection feature.

By default, the System State Protection feature is disabled. You can enable System State Protection while creating a new scenario, or configure System State Protection for existing scenarios using the Scenario Properties pane from the CA ARCserve Replication or High Availability Manager. System State Protection option also lets the user define a schedule for protecting the System State.

To configure system state protection using the scenario creation wizard; proceed with the typical scenario creation steps until you reach the Scenario Properties dialog. In the Scenario Properties dialog, under Replication, set System State Protection to ON. Click Set Schedule and set the schedule for taking system state snapshots, proceed with the scenario creation steps until you reach the Master and Replica Properties dialog. Expand Replication properties of the Replica server and set the Store System State on this Replica property to ON. Verify and Run the scenario to start System State Protection.

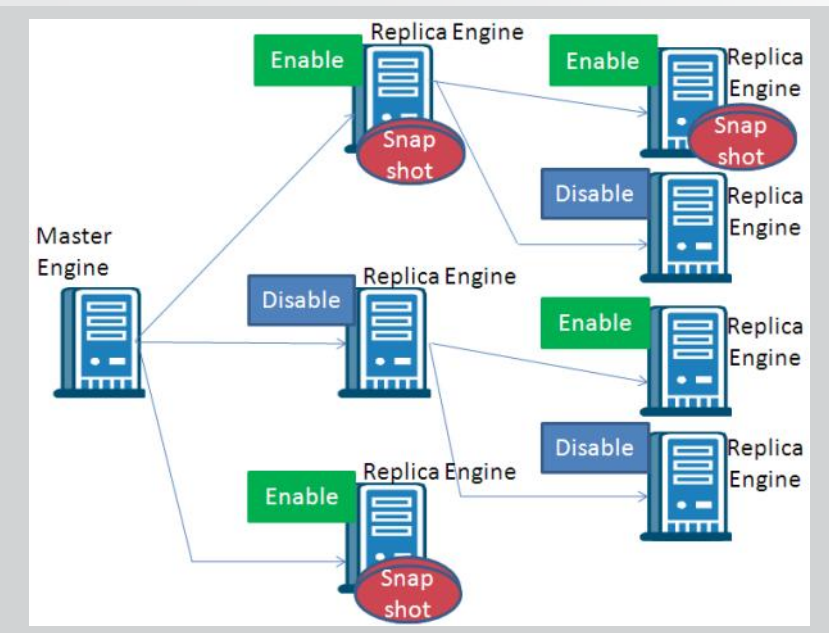
To configure system state protection for existing scenarios; from the CA ARCserve Replication or High Availability Manager, select the Scenario to change its System State Protection property. On the Scenario properties pane, expand the Replication node and set the Enable System State Protection node to ON and set the schedule. Similarly to configure the Replica server, select a Replica to enable its System State Protection property from the CA ARCserve Replication or High Availability Manager. On the Properties panel, expand the Replication node and set the Store System State on this replica node property to ON and then modify the Replica server storage property values as required.

How System State Protection Works

System State Protection does not depend on the server type; you can enable this feature in any scenario. When System State Protection is enabled on the Master server, the Master will copy the system state periodically and create snapshot files. The Snapshot file is transferred to all Replicas that are configured to receive the file. If there are more Replicas under any Replica, the Replica acts as a relay station. It transfers the file to Replicas configured under it just like the Master does. During transfer, only Replicas with the “Store System state on this replica” property enabled will keep the snapshot file locally. Those Replicas that have this property disabled will eventually delete the snapshot.

DURING REPLICATION

System State Protection enables you to choose the replicas on which you can store Master system state data, and the number of copies to keep on each replica server.



DURING RESTORE

Restoring System State data is similar to the usual recovery process; however, during restore you are prompted to select the Recovery Source.

During Restore, a new scenario is created in which the Master and Replica servers reverse roles. The scenario then transfers the System State snapshot to the original Master. User can restore application data and/or system state during recovery operation. CA ARCserve Replication and High Availability waits for application data recovery to complete first, including synchronization and then initiates the system state data recovery.

Frequently Asked Questions

Q: Do I need additional license to protect my system state data?

A: No, System State Data Protection feature comes along with the base product and does not need any additional license. You can enable protection to system state data during scenario creation or make changes to an existing scenario using the Scenario Properties pane from the CA ARCserve Replication or High Availability Manager.

Summary

CA ARCserve Replication and High Availability products are powerful, easy-to-use products that enable you to perform online replication and ensure high availability of your systems, applications and data. System State Protection lets you create a backup file for critical system related components such as boot files, COM+ Class Registration database, registry service and a host of other components depending on the operating system. The backup file can then be used to recover the critical system components in the event of a system failure.

For more information about the CA ARCserve Family of products, please visit arcserve.com/products or test drive our products at arcserve.com/software-trials.