

Microsoft Windows System State Recovery

<https://campus.barracuda.com/doc/79463668/>

A Microsoft Windows system state backup protects operating system files, enabling you to recover when a machine starts but you have lost system files and/or the registry. A system state backup includes the following:

- **Domain member** – Boot files, COM+ class registration database, registry
- **Domain controller** – Active Directory (NTDS), boot files, COM+ class registration database, registry, system volume (SYSVOL)
- **Machine running cluster services** – Additionally backs up cluster server metadata
- **Machine running certificate services** – Additionally backs up certificate data

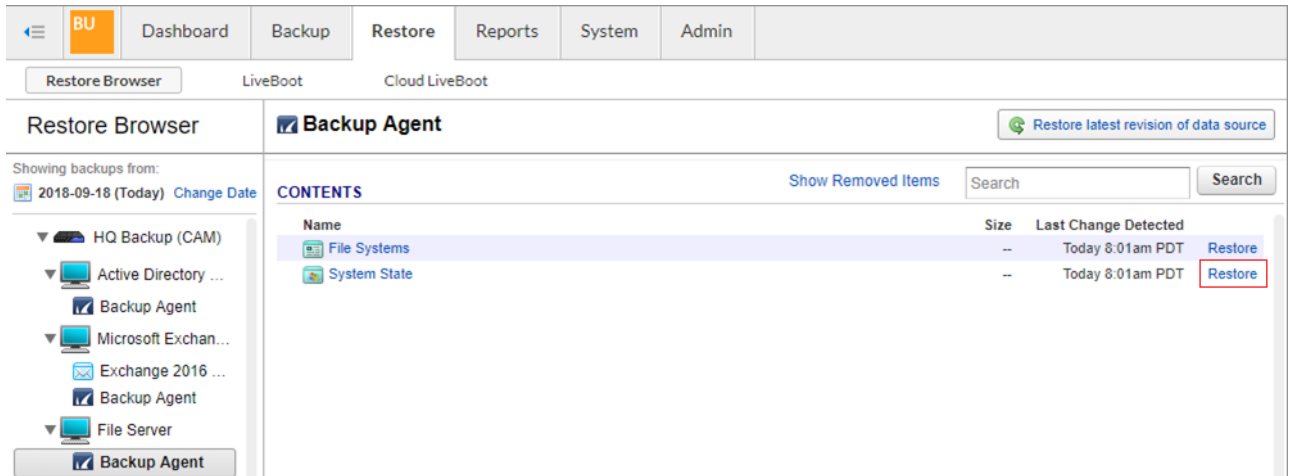
The Barracuda Backup system state restore performs a non-authoritative restore.

Incorrectly restoring the system state of a machine can make it unusable. Ensure that all troubleshooting and corrective options have been exhausted before attempting to restore the Windows system state.

Windows System State Restore

Use the following steps to perform a Windows system state restore:

1. Boot the server into Directory Services Restore Mode (DSRM).
 1. Restart the server.
 2. When the BIOS information appears, press **F8**.
 3. Select **Directory Services Restore Mode**, and press **Enter**.
 4. Log in by using the Directory Services Restore Mode password.
2. Log in to Barracuda Backup, and go to the **Restore > Restore Browser** page.
3. Select the data source you want to recover, navigate to the Backup Agent container, and click the **Restore** link next to the System State container:



Restore Browser | LiveBoot | Cloud LiveBoot

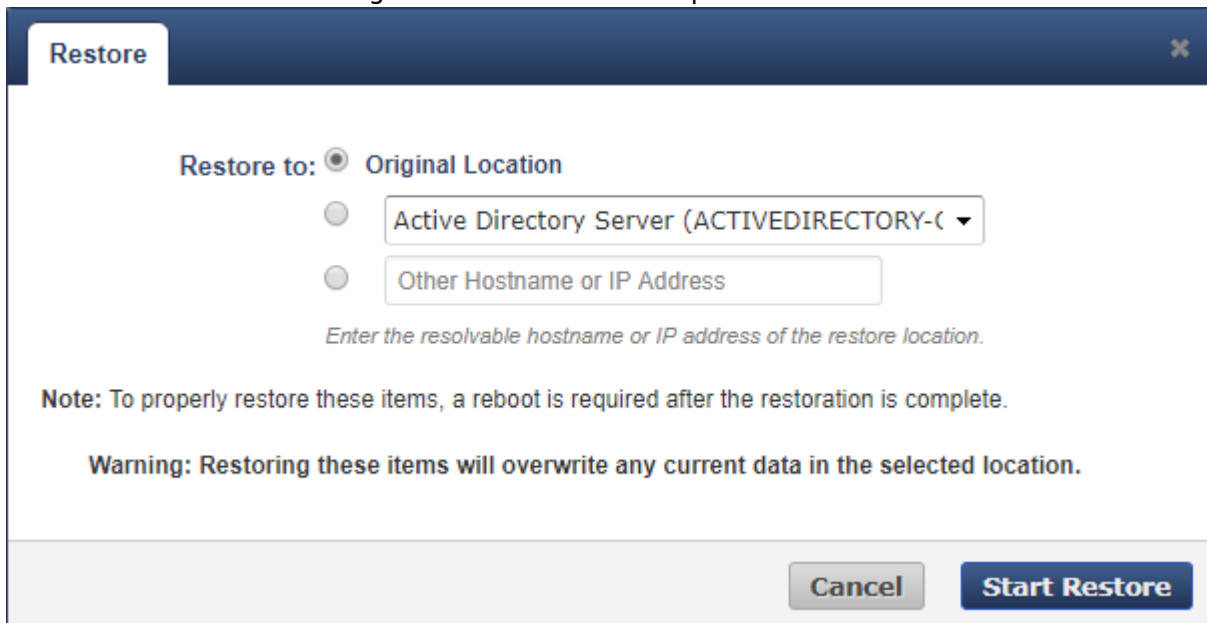
Restore Browser | **Backup Agent** | Restore latest revision of data source

Showing backups from: 2018-09-18 (Today) Change Date

CONTENTS

| Name | Size | Last Change Detected | |
|--------------|------|----------------------|---------|
| File Systems | -- | Today 8:01am PDT | Restore |
| System State | -- | Today 8:01am PDT | Restore |

- In the **Restore** dialog, select **Original Location**, or manually enter the Hostname or IP address if this information has changed since the last backup:



Restore

Restore to: Original Location

Active Directory Server (ACTIVEDIRECTORY-C)

Other Hostname or IP Address

Enter the resolvable hostname or IP address of the restore location.

Note: To properly restore these items, a reboot is required after the restoration is complete.

Warning: Restoring these items will overwrite any current data in the selected location.

Cancel Start Restore

- Click **Start Restore**.
- Go to the **Reports > Restore** page to monitor the progress of the restore job.
- When the restore job is complete, reboot the server normally.

Recover Microsoft Windows Active Directory

Before attempting to recover a domain controller, first review the following Microsoft TechNet articles for a complete list of recommendations:

- [Active Directory Backup and Restore](#)
- [Domain Controller Recovery](#)

Restoring a domain controller or Windows system state should only be used as a last resort or in a disaster recovery situation. Restoring the system state on a domain controller can have severe consequences.

Per Microsoft:

If there is a working domain controller in the infrastructure, you should recover from an Active Directory domain controller failure by building a new domain controller, joining it to the existing domain, and allowing Active Directory replication to update it to the current state.

The only time you should use domain controller backup images is when the failure has resulted in loss of all the domain controllers in the infrastructure or if one or more objects have been deleted from Active Directory by accident and need to be authoritatively restored.

To recover an entire Active Directory (AD) domain controller using bare metal recovery, see [Bare Metal Recovery](#).

To recover the system state of an AD domain controller, see the *Recover Microsoft Windows Active Directory* section above. This can be used to recover from AD data corruption. AD data corruption occurs when the directory contains corrupt data that has been replicated to all domain controllers or when a large portion of the AD hierarchy has been accidentally changed (such as deletion of an OU) and this change has replicated to other domain controllers.

Figures

1. SystemStateContainer.png
2. SelectOriginalLocation.png

© Barracuda Networks Inc., 2019 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.