
FORESCOUT

Forescout
eyeRecover
Service continuity and resiliency
for single- or multi-site deployments

eyeRecover

Highlights

Failover Clustering

How Failover Clustering works

eyeRecover Datasheet

Service continuity and resiliency for single- or multi-site deployments

Thank you for downloading this Forescout datasheet. Carahsoft is the dealer and distributor for Forescout cybersecurity solutions available via GSA Schedule 70, NASA SEWP V, ITES-SW, and other contract vehicles.

To learn how to take the next step toward acquiring Forescout's solutions, please check out the following resources and information:

For additional resources:
carah.io/ForescoutResources

For upcoming events:
carah.io/ForescoutEvents

For additional Forescout solutions:
carah.io/ForescoutProducts

For additional Cybersecurity solutions:
carah.io/Cybersecurity

To set up a meeting:
Forescout@carahsoft.com
833-FSCT-GOV

To purchase, check out the contract vehicles available for procurement:
carah.io/ForescoutContracts

For more information, contact Carahsoft or our reseller partners:
Forescout@carahsoft.com | 833-FSCT-GOV

Forescout eyeRecover

Service continuity and resiliency for single- or multi-site deployments

The Forescout platform can be deployed on physical or virtual appliances on your network to provide device visibility and control across your extended enterprise. These critical security functions rely on the availability and uptime of Forescout services—any extended interruption can compromise your security posture and impact business operations.

As with any critical service, you need to consider deployment architectures that are resilient to system failures, site-wide disruptions and natural or human-induced disasters. Planning and implementing a recovery strategy reduces downtime and enables continuity of vital business and security systems. Forescout eyeRecover provides automated failover, resiliency and service continuity for Forescout deployments with a choice of active/standby high-availability pairing or failover clustering capabilities.

Highlights

- Provide resiliency and high availability for Forescout deployments
- Reduce risk of business disruption and downtime
- Protect against system, network or site-wide failures
- Help meet IT service continuity mandates
- Automate failover and intelligent reallocation of workloads
- Enable cross-site failover for disaster recovery scenarios
- Perform manual failover to facilitate maintenance procedures and upgrades
- Support centralized and distributed Forescout deployments

Failover Clustering

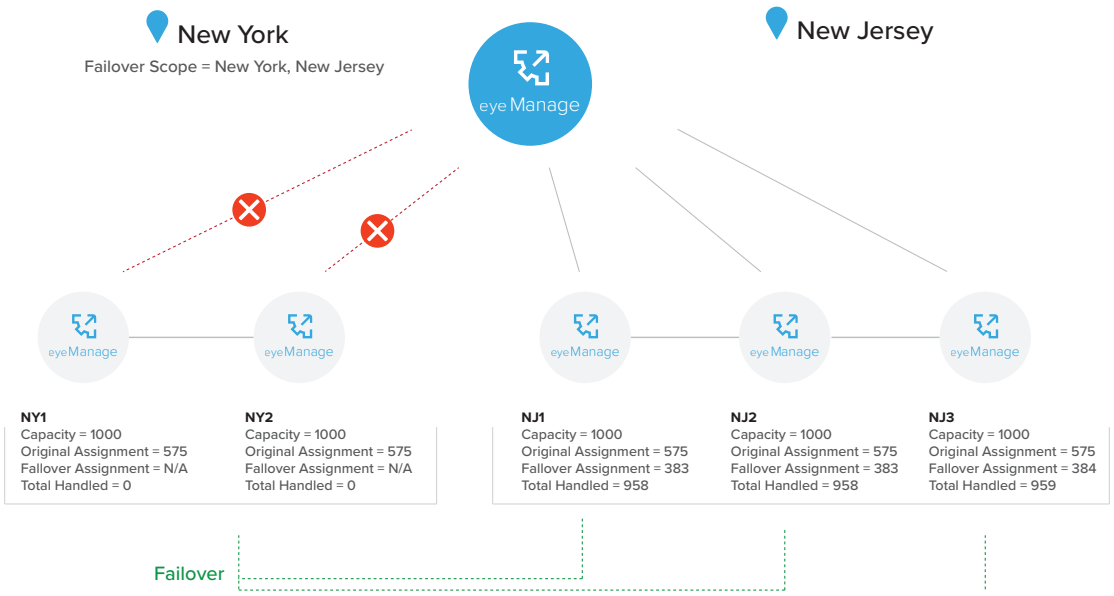
Most Forescout deployments involve multiple physical or virtual appliances, sometimes distributed across several sites. Each appliance can provide a range of services—device visibility, posture assessment, access control and policy enforcement—for a number of endpoints. Failover clusters harness the unallocated processing capacity in these appliances to provide service resiliency without the added cost and complexity of idle, standby appliances.

With failover clustering, you can create logical groups of appliances and implement an automated process for reallocating the workload(s) of one or more failed nodes, a cluster or even an entire site. Clusters can provide resiliency for centralized or distributed deployments and can be deployed in single- or multi-site environments.

How Failover Clustering works

Deployments should be planned in such a way that appliances have extra capacity to receive the anticipated failover workload (the failover assignment) in addition to their own normal workload (the original assignment). When an appliance, a cluster or a site fails, its workload is transferred to and its load is balanced across the assigned receiving appliances. Failback occurs once a failed appliance or cluster recovers, at which point it regains the management of endpoints and network devices previously transferred to the recipient appliances.

Figure 1: Failover clustering in a multi-site scenario.



Cross-Cluster and Cross-Site Failover

In addition to failover and workload distribution between appliances within a single cluster, you can also configure failover scope to extend resilience across multiple clusters and locations. When an appliance fails, its workload is first distributed to other nodes within the cluster that have capacity. When all in-cluster capacity is allocated, workloads are then distributed to appliances in other clusters in the failover scope. This also enables cross-site failovers in the event of an entire cluster or site failure for disaster recovery purposes. See Figure 1.

High-Availability Pairing

Active/standby high-availability is implemented as a one-to-one pairing of appliances. One appliance is designated as a primary node, the other as a backup or secondary node. The two appliances are co-located and are synchronized by a pair of redundant, directly interconnecting cables.

To achieve redundancy, the primary node is set to manage activities required for device visibility and control. In the event that the primary node fails, the secondary node automatically takes over the required functions from the primary. When the primary node recovers, the backup node can be set to failback, restoring the original workload to the primary node.

FORESCOUT

Forescout Technologies, Inc.
190 W Tasman Dr.
San Jose, CA 95134 USA

Toll-Free (US) 1-866-377-8771
Tel (Intl) +1-408-213-3191
Support +1-708-237-6591

Learn more at Forescout.com